Nebraska Law Review

Volume 90 | Issue 4 Article 1

2012

When Rummaging Goes Digital: Fourth Amendment Particularity and Stored E-Mail Surveillance

Nicole Friess
Davis Graham & Stubbs LLP, nicole.friess@dgslaw.com

Nicole Friess*

When Rummaging Goes Digital: Fourth Amendment Particularity and Stored E-Mail Surveillance

TABLE OF CONTENTS

* Associate, Davis Graham & Stubbs LLP; LL.M., Information Technology and Intellectual Property, University of Colorado Law School, 2011; J.D., University of Colorado Law School, 2010; B.A., Political Economics, Barnard College, 2006. I would like to give many thanks to my mentor Paul Ohm for his guidance, as well as to my parents, Betsy and Michael Friess, for their unwavering love and support.

I. INTRODUCTION

Perhaps nothing is more akin to our innermost secrets than the content of our private conversations.[1] Conversational content, though, is no longer fleeting—millions of Americans use e-mail as a central medium of communication, their conversations preserved on the servers of internet service providers (ISPs).[2] Consider the contents of a typical e-mail account: It often contains e-mails to family, friends, and lovers with pictures, receipts, and appointments, and its contents may date back days or possibly even years. Also consider how invasive it would be if a police officer had unfettered access to that e-mail account and rifled through each and every stored e-mail and file.

The framers of our Constitution "sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations" and "conferred, as against the government, the right to be let alone."[3] The laws that govern government access to our private lives impose checks and balances on the power of the police to search and seize private information, protecting us from invasions of privacy unless an intrusion is justified by factual circumstance. When police investigate a crime and want to search for evidence, they must—in order to first obtain a search warrant—convince a magistrate judge that the facts known establish there is probable cause to believe a search will uncover evidence of wrongdoing.[4] However, a warrant based upon probable cause is not the only thing required for a search and seizure to be considered constitutional—the Fourth Amendment categorically prohibits the issuance of warrants except those *particularly describing* both the place to be searched and the things to be seized.[5] According to the Supreme Court:

> The manifest purpose of this particularity requirement was to prevent general searches. By limiting the authorization to search to the specific areas and

1. *See* Berger v. New York, 388 U.S. 41, 63 (1967) (referring to conversation as "the innermost secrets of one's home or office . . ."); United States v. Cox, 449 F.2d 679, 686 (10th Cir. 1971) ("[A] search for property is a different and less traumatic invasion than is the quest for private conversations.").
2. Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1423 (2009). An ISP owns points on a network between a user's computer and the rest of the internet. *Id.* Its principal role is to route internet traffic by receiving communications from its users and sending them to the rest of the world, and vice versa, over cables between its facilities and the premises of its users. *Id.* All of a user's communications must pass through an ISP. *Id.*
3. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).
4. *See, e.g.*, Jones v. United States, 362 U.S. 257, 271 (1960).
5. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

> things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the [f]ramers intended to prohibit.[6]

However, the extent to which the Fourth Amendment protects the content of stored e-mail communications is an open question—a new frontier in Fourth Amendment jurisprudence that has been little explored.[7] Many have addressed the issues surrounding probable cause and stored e-mail surveillance,[8] yet neither Congress nor courts or scholars have addressed how the particularity requirement should apply in this context. Simply stated, how warrants authorizing stored e-mail surveillance describe with particularity both the place to be searched and the things to be seized has been greatly overlooked.

A central purpose served by the particularity requirement is the prevention of "general, exploratory rummaging in a person's belongings."[9] The potential for such boundless rummaging is significantly magnified in the internet age, as one's private, digital conversations so infrequently remain within the periphery of one's own control.[10] Congress has codified procedural protections derived from the particularity requirement[11] that protect privacy and curtail abuse for *some* forms of electronic surveillance, especially when such surveillance divulges a wide range of private information over a significant period of

---

6. Maryland v. Garrison, 480 U.S. 79, 84 (1987).
7. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904, 910–11 (9th Cir. 2008), *rev'd and remanded by* City of Ontario v. Quon, 130 S. Ct. 2619 (2010).
8. *See* Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-Mail*, 2008 U. CHI. LEGAL F. 121, 175–76 (2008) (advocating for probable-cause based warrants for all stored communications); Orin Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1041–44 (2010) (arguing that permitting the government to obtain stored communications without probable cause is unconstitutional); Paul Ohm, *Probably Probable Cause: The Diminishing Importance of Justification Standards*, 94 MINN. L. REV. 1514, 1516 (2010) (discussing the application of probable cause and other justification standards online); Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1299 (2004) (arguing that "for most uses of electronic surveillance, warrants supported by probable cause should be required").
9. Andresen v. Maryland, 427 U.S. 463, 480 (1976).
10. *See* United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 313 (1972) ("[T]he broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards.").
11. *See, e.g.*, Wiretap Act, 18 U.S.C. §§ 2510–2522, 2518(1)–(5) (2006 & Supp. III 2009); Berger v. New York, 388 U.S. 41, 58–60 (1967); Katz v. United States, 389 U.S. 347, 355–56 (1967); *see also* Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶ 54 (2007) ("[W]e want to make clear our view that a warrant for television surveillance that did not satisfy the four provisions of [the Wiretap Act] that implement the Fourth Amendment's requirement of particularity would violate the Fourth Amendment." (citing United States v. Torres, 751 F.2d 875, 883–85 (7th Cir. 1984))).

time.[12] However, the statutory laws governing the surveillance of stored e-mails and files do not contain these same protections.

The privacy invasions that result when particularity is lacking in the context of stored e-mails and files are best demonstrated by example. Imagine that Bob is the sole owner of a company that markets and sells its products through telephone orders, online sites, and retail stores. Bob's customers, however, are angry. They file a criminal complaint against Bob and his company, claiming the products they purchased do not work as advertised and their money-back guarantees have not been honored. The government then starts investigating Bob and his company in connection with the marketing and sale of the products, trying to find violations of federal law, such as mail fraud or money laundering.

Bob has an e-mail account through which both his professional and personal e-mails are stored on a server, owned and operated by his ISP. The government wants to know if these e-mails contain leads or evidence, so it obtains a court order under the Stored Communications Act (SCA)[13] to compel the ISP to divulge the e-mails. Pursuant to the SCA, the court order grants government access to Bob's e-mail subscriber information and the contents[14] of all Bob's e-mails that have been in storage for more than 180 days.[15] The ISP divulges the e-mails to the government—every e-mail more than 180 days old from the time Bob first opened his e-mail account—except e-mails that Bob did not access, view, or download. The government examines thousands of these e-mails, many of which are deeply personal and completely unrelated to Bob's business, having no relevance to the government's investigation. As permitted under the SCA, moreover, the ISP is forbidden from notifying Bob the government has gained access to his e-mails.[16]

Based on the information provided by the complaining customers, the government knows specific information concerning when and how

12. *See Berger*, 388 U.S. at 58–60, 63–64 (invalidating a New York statute under the Fourth Amendment because it authorized electronic eavesdropping without procedural safeguards); *Katz*, 389 U.S. at 347 (extending Fourth Amendment protections beyond physical intrusions); *see also* Freiwald, *supra* note 11, ¶¶ 53–54 (noting seven federal appellate courts hold the Fourth Amendment regulates silent video surveillance in the same heightened manner as wiretapping).
13. 18 U.S.C. §§ 2701–2711.
14. *Id.* § 2703(c)(2). As to e-mail subscriber information, the government may compel an ISP to disclose the name, address, length of service (including start date and types of service utilized), subscriber number or identity (including e-mail addresses and IP addresses), and means or source of payment for service (including any credit card or bank account number). *Id.* "Content" of is defined as "any information concerning the substance, purport, or meaning of that communication." *Id.* § 2510(8).
15. *Id.* § 2703(a)–(d).
16. *Id*. § 2705.

the alleged federal offenses occurred. Yet the government never establishes probable cause to believe the search of Bob's stored e-mails will yield evidence of a crime, and it never obtains a warrant or attempts to limit its search to e-mails pertaining concerning only Bob's business. Nor does it limit its search and seizure to e-mails sent or received during the time period when the alleged federal offenses occurred. The government does not do any of these things, even though it could, because the SCA does not require it to do so.[17] Is it possible the government can search and seize thousands of Bob's personal, private e-mails which have no relevance to its investigation? Yes, it is possible. In fact, the scenario just described is similar to what happened to Steven Warshak in 2005.[18] Such government surveillance unreasonably intrudes into our online personal privacy and dignity. This stems from the failure of the courts to, until recently, extend the Fourth Amendment's protections to e-mail communications.[19]

To date, most of the discussion regarding how the Constitution protects privacy interests in stored e-mail has focused on whether a warrant is required to conduct stored e-mail surveillance and whether probable cause is the appropriate justification standard .[20] Little to no attention has been directed toward how the particularity requirement of the Fourth Amendment applies to searches and seizures of stored e-mail communications.[21] Only Susan Freiwald has argued that procedural particularity should be required in order for government acquisitions of stored e-mails to pass constitutional muster, yet she did not enumerate specific standards of particularity.[22] This Article addresses how the particularity requirement applies to stored e-mail surveillance and sets forth standards to evaluate the particularity of search warrants for stored e-mail communications.

This Article proceeds in four parts. Part II explains why and how procedural protections derived from the particularity requirement have been codified by Congress and imposed by the courts in order to limit certain electronic-surveillance techniques. Part III describes how probable cause defines which stored e-mails the government may

17. *Id*. § 2703(b), (d) (describing the requirements to obtain an administrative subpoena and a "d-order" to compel disclosure of contents of stored e-mail, respectively).
18. United States v. Warshak, 631 F.3d 266, 283 (6th Cir. 2010).
19. *Id.* at 288 (holding "to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional").
20. *See, e.g.*, Bellia & Freiwald, *supra* note 8, at 175–76; Solove, *supra* note 8, at 1299.
21. Courts have recognized and struggle with the uncertainty as to the precise applicability of the Fourth Amendment's particularity requirement with respect to searches and seizures of e-mail communications. *See, e.g.*, United States v. Taylor, 764 F. Supp. 2d 230, 233–35 (D. Me. 2011); United States v. Bowen, 689 F. Supp. 2d 675, 681 (S.D.N.Y. 2010).
22. *See* Freiwald, *supra* note 11, ¶¶ 1–4.

search and seize and the reason why scholarship has overemphasized probable cause in the context of stored e-mail surveillance. Then described is how current statutory law governing stored e-mail surveillance is in disharmony with the Fourth Amendment, and therefore how it must be amended to require search warrants for stored e-mail surveillance. Part IV proposes concrete standards for determining whether a warrant authorizing a search and seizure of stored e-mail communications adheres to the particularity requirement of the Fourth Amendment. Finally, Part V addresses the practicalities of the proposed particularity standards and responds to several potential objections concerning the implementation of these standards.

II. EXTENDING THE FOURTH AMENDMENT—FROM TELEPHONES TO E-MAIL

Great tension exists between privacy and security.[23] The government promotes security by investigating crimes. In a digital world, criminal investigations involve increasingly intrusive monitoring and information gathering, which pose substantial threats to privacy. Indeed, there is a deep-seated unease and apprehension that the government uses electronic surveillance "to intrude upon cherished privacy of law-abiding citizens."[24] Between the governmental need to investigate crimes and the societal need to protect personal privacy stands the Fourth Amendment—the constitutional balancing factor.[25] It safeguards the privacy of individuals against arbitrary invasions by the government.[26]

The government's surveillance techniques and technologies are constantly evolving to keep pace with revolutions in communication. Interpretation of whether government surveillance is reasonable under the Fourth Amendment continually evolves in order to address constitutional privacy concerns previously unforeseen.[27] Long before

23. *See, e.g.*, New Jersey v. T.L.O., 469 U.S. 325, 337 (1985) ("On one side of the balance are arrayed the individual's legitimate expectations of privacy and personal security; on the other, the government's need for effective methods to deal with breaches of public order."); United States v. Farlow, No. CR-09-38-B-W, 2009 WL 4728690, at *5 (D. Me. Dec. 3, 2009) ("With the advent of the computer age, courts have struggled to balance privacy interests against law enforcement interests.").
24. United States v. U.S. District Court (*Keith*), 407 U.S. 297, 312 (1972).
25. *See* Schmerber v. California, 384 U.S. 757, 767 (1966) ("The overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State.").
26. Camera v. Mun. Ct., 387 U.S. 523, 528 (1987); *see* Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602, 613–14 (1989) ("The [Fourth] Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government or those acting at their direction.").
27. *See* United States v. Warshak, 631 F.3d 266, 285 (6th Cir. 2010) ("[T]he Fourth Amendment must keep pace with the inexorable march of technological progress,

the advent of e-mail, the telephone revolutionized communication by exponentially increasing our ability to connect. In response to this new technology, recording and transmitting devices were invented, thereby enabling the government to hear our telephone conversations without detection. When confronted with the constitutionality of these new surveillance techniques, the Supreme Court held that wiretapping necessitated implementation of Fourth Amendment privacy safeguards given the telephone's vital role as a medium for communication[28] as well as the private nature of telephone conversations.[29] Seven federal appellate courts have used a similar rationale to extend analogous protections concerning the government's use of silent video surveillance.[30]

These two methods of electronic surveillance share common characteristics. The surveillance is hidden—wiretaps and video cameras go unseen and unnoticed by those under surveillance.[31] The surveillance is intrusive in that it captures the private conversations and actions of the investigation target, and it is indiscriminate in that it "does not merely disclose the target's incriminating information, but also the target's non-incriminating information as well as information about those innocent parties."[32] Lastly, it is continuous because, in comparison to a one-shot search, wiretapping and video surveillance collect information over an extended period of time.[33]

Since the advent of e-mail, an explosion of internet-based communication has taken place, with telephone calls and postal mail waning in importance.[34] E-mail accounts generally contain thousands of

---

or its guarantees will wither and perish." (citing Kyllo v. United States, 533 U.S. 27, 34 (2001))); United States v. Hill, 459 F.3d 966, 979 (9th Cir. 2006) ("Technology is rapidly evolving and the concept of what is reasonable for Fourth Amendment purposes will likewise have to evolve.").

28. Katz v. United States, 389 U.S. 347, 352 (1967).
29. Berger v. New York, 388 U.S. 41, 58–60 (1967) (holding state's electronic eavesdropping statute facially unconstitutional for lack of adequate Fourth Amendment safeguards); *Katz*, 389 U.S. at 347 (finding a Fourth Amendment expectation of privacy in telephone calls made from a closed phone booth).
30. *See* Freiwald, *supra* note 11, ¶¶ 53–54.
31. *Id*. ¶ 53–54 & n.80 (citing United States v. Torres, 751 F.2d 875, 877 (7th Cir. 1984) (describing the use of television cameras in the homes of suspected terrorists in 1983)).
32. *See, e.g.*, United States v. Torres, 751 F.2d 875, 878 (7th Cir. 1984) (noting that video surveillance and recording conversations are invasions of privacy); Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 80 (2004).
33. Freiwald, *supra* note 32, at 80.
34. United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010); *see also* Lauren Reardon, *Email Statistics Report, 2009–2013*, THE RADICATI GRP., INC. (May 6, 2009), http://www.radicati.com/wp/wp-content/uploads/2009/05/e-mail-statistics-report-2009-pr.pdf (estimating there were 1.4 billion e-mail users worldwide and 47 billion non-spam e-mail messages sent daily in 2009).

other messages among which the sought-after communication may be stored or concealed.[35] ISPs offer a variety of e-mail services to their users, many of which are web-based accounts maintained by the ISPs.[36] E-mails sent, received, archived, and even deleted via such e-mail accounts are often stored on the ISP's mail servers for varying lengths of time.[37] Advances in government surveillance as well as increasing data retention capabilities[38] pose serious threats to individual privacy without procedural constraints.[39]

Surveillance of stored e-mail shares the same characteristics as wiretapping and silent video surveillance and thus exhibits the same constitutional infirmities.[40] Stored e-mail surveillance is hidden in several ways.[41] ISPs are intermediaries between e-mail-account holders and the government—ISPs can access e-mails stored on their servers pursuant to a request by law enforcement without knowledge of the account holder.[42] The government may also specifically request that ISPs delay notifying the account holder after the ISP has ac-

35. *See Warshak*, 631 F.3d at 284–85.

36. Some of the largest e-mail services offer users huge amounts of computer disk space to warehouse their e-mails for perpetual storage. For example, Google's "Gmail" service offers more than seven gigabytes of free storage space. *How it Works*, GOOGLE.COM, http://mail.google.com/support/bin/answer.py?hl=en&answer=39567 (last updated Oct. 4, 2011). Google also encourages its users not to throw messages away. *Getting Started with Gmail*, GOOGLE.COM, http://mail.google.com/mail/help/intl/en/start.html (last visited Oct. 26, 2011) ("Don't waste time deleting . . . . [T]he typical user can go years without deleting a single message.").

37. LEONARD DEUTCHMAN & SEAN MORGAN, AM. PROSECUTORS RESEARCH INST., THE ECPA, ISPS & OBTAINING E-MAIL: A PRIMER FOR LOCAL PROSECUTORS 10 (2005).

38. Recently, the Department of Justice renewed calls for legislation mandating a minimum data retention period for ISPs. *Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes, Hearings before the H. S. Comm. on Crime, Terrorism, and Homeland Sec.*, 112th Cong. 6–8 (2011) (statement of Jason Weinstein, Deputy Assistant Att'y Gen., Criminal Division, Department of Justice). Recent proposals also urge online sites or services that allows users to communicate (such as blogs, social networks, and e-mail services) to track and retain data about every communication that any user makes online. *Id.* at 34–35 (statement of John B. Morris, Jr., General Counsel, Center for Democracy and Technology).

39. *See, e.g.*, Berger v. New York, 388 U.S. 41, 62 (1967) ("[T]he fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual; . . . indiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments . . . ." (quoting Lopez v. United States, 373 U.S. 427, 441 (1963))).

40. Freiwald, *supra* note 11, ¶¶ 62–70.

41. *Id.* ¶¶ 62–63.

42. United States v. Bach, 310 F.3d 1063, 1066–67 (8th Cir. 2002) (finding an ISP's execution of a search warrant constitutional because the Fourth Amendment "does not explicitly require official presence during a warrant's execution, therefore it is not an automatic violation if no officer is present during a search" (citing Wilson v. Arkansas, 514 U.S. 927, 931–34 (1995))).

cessed stored e-mail communications.[43] Stored e-mail surveillance is indiscriminate in that current law permits the government to seize stored e-mails without limitations as to the time frame, the parties to the communication, or the subject matter of the communication, which almost certainly results in the disclosure of information pertaining to innocent individuals and activities.[44] It is continuous without constraints because the government can acquire stored e-mails spanning indefinite periods of time.[45] The risk of exposing intimate and innocent correspondence when searching and seizing stored e-mails is thus magnified given the hundreds or even thousands of emails associated with a single e-mail account.[46]

Perhaps most importantly, stored email surveillance can be extraordinarily intrusive. The Supreme Court in *Smith v. Maryland*[47] held the Fourth Amendment does not extend to the government's use of pen registers, which record the numbers dialed on a telephone. In so holding, the Court noted the "limited capabilities" of the pen register and the limited nature of the information elicited from a pen register.[48] Unlike wiretaps, which record the contents of conversations, the government does not obtain the purport of communications between a caller and the recipient, or their respective identities from pen-register surveillance.[49] It was these characteristics that rendered pen-register surveillance less intrusive than wiretapping for purposes of the Court's Fourth Amendment analysis.[50] By way of analogy, courts have generally declined to extend Fourth Amendment protection to internet subscriber information.[51]

43. 18 U.S.C. § 2705 (2006 & Supp. III 2009).

44. Freiwald, *supra* note 11, ¶ 68; *see* United States v. Mesa-Rincon, 911 F.2d 1433, 1442–43 (10th Cir. 1990); United States v. Torres, 751 F.2d 875, 885 (7th Cir. 1984).

45. *Torres*, 751 F.2d at 884 (finding that electronic surveillance is "by nature a continuing rather than one-shot invasion" and "is even less discriminating than a physical search, because it picks up private conversations (most of which will usually have nothing to do with any illegal activity) over a long period of time"); Freiwald, *supra* note 11, ¶ 70.

46. *See* United States v. Warshak, 631 F.3d 266, 284–85 (6th Cir. 2010).

47. 442 U.S. 735 (1979).

48. *See id.* at 741.

49. *Id*. (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 167 (1977)).

50. *See id.*

51. *See, e.g.*, Rehberg v. Paulk, 611 F.3d 828, 842–47 (11th Cir. 2010) (summarizing case law holding Fourth Amendment does not extend to non-content information), *cert. granted*, 131 S. Ct. 1678 (2011); United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010) (holding individuals do not have protectable expectation of privacy in electronic subscriber information); United States v. Perrine, 518 F.3d 1196, 1204–05 (10th Cir. 2008) (explaining Fourth Amendment protection does not extend to subscriber information sent to Yahoo!); United States v. Forrester, 512 F.3d 500, 509–11 (9th Cir. 2008) (finding no privacy interest in non-content information by way of analogy to telephone numbers).

In contrast, searches and seizures of the *content* of stored e-mail is *more* intrusive than wiretapping or video surveillance because e-mails typically contain more personal and sensitive information—which touches on many private aspects of life—than do analogous phone conversations or silent videos.[52] In *Warshak v. United States*,[53] the Sixth Circuit emphasized the large amount of information that e-mail accounts often contain:

> People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button. Commerce has also taken hold in email. Online purchases are often documented in email accounts, and email is frequently used to remind patients and clients of imminent appointments. In short, "account" is an apt word for the conglomeration of stored messages that comprises an email account, as it provides an account of its owner's life.[54]

The Supreme Court also recently acknowledged in *City of Ontario v. Quon*[55] that certain technologies may be "so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression," which "strengthen[s] the case for an expectation of privacy."[56] The case for Fourth Amendment protections for stored e-mail is inherently strong as e-mail is "the technological scion of tangible mail, and it plays an indispensable part in the [i]nformation [a]ge."[57] Although the Court indicated particularly pervasive technologies, such as e-mail, may present a strong case for constitutional protections, the Court side-stepped the issue of whether and when the Fourth Amendment protects electronic communications.[58]

E-mail is as important to Fourth Amendment principles today as protecting telephone conversations was in the past.[59] Its pervasiveness as a central medium of communication has significantly heightened online privacy concerns—the government can peer deeply into the corners of an individual's private life to a greater degree than ever before by obtaining access to the contents of the individual's e-mail

52. *See* United States v. Lucas, 640 F.3d 168, 178 (6th Cir. 2011) ("[T]here is a far greater potential for . . . a consequent invasion of privacy when police execute a search for evidence on a computer."); Freiwald, *supra* note 11, ¶ 66.
53. 631 F.3d 266 (6th Cir. 2010).
54. *Id.* at 284.
55. 130 S. Ct. 2619 (2010).
56. *Id*. at 2630.
57. *Warshak*, 631 F.3d at 286.
58. *Quon*, 130 S. Ct. at 2629 (stating that in *Katz*, "the Court relied on its own knowledge and experience to conclude that there is a reasonable expectation of privacy in a telephone booth" but noting that *Katz* acknowledged it was "not so clear that courts . . . are on so sure a ground" as to electronic devices).
59. *See* Katz v. United States, 389 U.S. 347, 352 (1967) ("To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.").

account.[60] A focused look into the invasive nature of stored e-mail surveillance, and the excessive privacy intrusions that result if such surveillance is not kept in check,[61] compels the conclusion that surveillance of stored e-mails and files must comport with the Fourth Amendment. The few appellate opinions to consider the issue seem to agree.[62] The Sixth Circuit now recognizes that the Fourth Amendment extends to e-mails "that are stored with, or sent or received through, a commercial ISP."[63] Courts will likely follow the Sixth Circuit's lead and acknowledge that a constitutionally-protected privacy right in the contents of e-mail communications exists, thereby recognizing that e-mail surveillance excessively intrudes on privacy rights and is susceptible to abuse without adequate oversight.[64] As a result, the textual components of the Fourth Amendment govern the constitutionality of stored e-mail surveillance.

III. SCHOLARLY AND STATUTORY RESPONSES TO STORED E-MAIL SURVEILLANCE

The constitutionality of government surveillance is judged against the Fourth Amendment's general rule of reasonableness—the Amendment prohibits "unreasonable searches and seizures."[65] Reasonableness is determined by balancing the government's need to search or seize against the invasion which the search or seizure entails.[66] A search or seizure of stored e-mail will be considered constitutional if "reasonable" and unconstitutional if "unreasonable," but what defines reasonableness? The answer is a combination of Fourth Amendment rules and presumptions that are designed to control the conduct of government officials who may significantly intrude upon privacy interests.[67]

60. *See id*.

61. *See* Freiwald, *supra* note 11, ¶¶ 21, 51; Ohm, *supra* note 8, at 1558.

62. *E.g.*, Rehberg v. Paulk, 611 F.3d 828, 842–47 (11th Cir. 2011) (finding the application of the Fourth Amendment to e-mail content is not clearly established and therefore qualified immunity was appropriate); Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904, 910–11 (9th Cir. 2008), *rev'd and remanded by* City of Ontario v. Quon, 130 S. Ct. 2619, 2629–33 (2010).

63. United States v. Lucas, 640 F.3d 266, 288 (6th Cir. 2011) (citing United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010)).

64. *See* Freiwald, *supra* note 11, ¶¶ 71–72.

65. U.S. CONST. amend. IV; Illinois v. McArthur, 531 U.S. 326, 330 (2001) (citing Texas v. Brown, 460 U.S. 730, 739 (1983)).

66. Terry v. Ohio, 392 U.S. 1, 20–21 (1968).

67. *Id*.

A. Overemphasizing the Probable Cause Warrant

One such rule of reasonableness holds that a warrant is required before the government can conduct searches and seizures.[68] As the Supreme Court noted in the context of telephone surveillance, the Fourth Amendment's warrant requirement does "not vanish when the search in question is transferred from the setting of a home, an office, or a hotel room to that of a telephone booth."[69] Thus, an electronic device, used without trespass onto any given enclosure, is a search for which a Fourth Amendment warrant is needed.[70] As Orin Kerr notes, the Court's "forceful rejection of a warrant exception for telephone bugging seems to extend naturally to the [i]nternet" as it is difficult to articulate why searches and seizures of internet communications, such as e-mail, might justify treatment different from audio-bugging a telephone booth.[71]

To justify the issuance of a warrant for the contents of stored e-mails, the government is required to establish probable cause to search and seize those contents. To do so, the government must establish a "fair probability" under the totality of the circumstances[72] that the e-mails sought contain contraband, evidence of a crime, fruits of a crime, or the instrumentality of a crime.[73] According to the Supreme Court, the probable cause standard is satisfied by an affidavit that establishes "a fair probability that contraband or evidence of a crime will be found in a particular place."[74]

Probable cause will not exist if the government can only point to a "bare suspicion" that criminal evidence will be found in the place searched.[75] Probable cause serves to guarantee a substantial probability that the privacy invasions resulting from surveillance will be justified by discovery of offending items.[76] Yet as Paul Ohm notes, it is increasingly common that "whenever the police have any suspi-

68. Absent a few specifically established and well-delineated exceptions which generally do not apply to electronic surveillance. *See* Katz v. United States, 389 U.S. 347, 357–58 (1967) ("It is difficult to imagine how any of those exceptions could ever apply to the sort of search and seizure involved in this case.").
69. *Id.* at 359.
70. United States v. White, 401 U.S. 745, 758 (1971) (Douglas, J., dissenting) (citing Katz v. United States, 389 U.S. 347 (1967)).
71. Kerr, *supra* note 8, at 1042–43.
72. Illinois v. Gates, 462 U.S. 213, 238 (1983).
73. *See* FED. R. CRIM. P. 41(c); COMPUTER CRIME & INTELLECTUAL PROP. SECTION, DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 63 (3d ed. 2009), [hereinafter CCIPS SEARCH-AND-SEIZURE MANUAL].
74. *Gates*, 462 U.S. at 238.
75. Brinegar v. United States, 338 U.S. 160, 175 (1949).
76. *E.g.*, United States v. Button, 653 F.2d 319, 321 (8th Cir. 1981); Comment, *Search and Seizure in the Supreme Court: Shadows on the Fourth Amendment*, 28 U. CHI. L. REV. 664, 690 (1961).

cion at all about a piece of evidence, they almost always have probable cause."[77] Supporting this argument is the technological architecture of the internet and the substance of court opinions addressing the issue.[78]

During an investigation the government pursues any and all digital, evidentiary leads, which turn out to be either "gold mines or dead ends, rarely something in between."[79] Suspicion therefore oscillates between probable cause and nothing at all.[80] Here is a common scenario: Investigators learn that an individual has been using an internet protocol (IP) address to commit a crime. Perhaps they obtain copies of incriminating e-mails—the messages are rich in leads toward identifying the sender, "most importantly in the message headers like the 'To' and the 'Received' lines that show the path taken across the [i]nternet."[81] Whether they have the individual's IP address or e-mail address (or other identifying handle), the investigators can subpoena the ISP associated with that IP address or e-mail account and obtain the individual's name and home address.[82] A government affidavit that describes such an investigation is typically sufficient to establish probable cause to obtain a traditional search warrant.[83]

While probable cause will look different in every case, empirical evidence compels the conclusion that the government either has probable cause or no suspicion at almost every stage of almost every internet investigation.[84] Court opinions have never held the government lacked probable cause to investigate an e-mail address or an IP address.[85] This even includes the few cases calling online surveillance into question.[86] Consequently, it follows that in the context

77. Ohm, *supra* note 8, at 1515.

78. *Id.* at 1525.

79. *Id.* at 1527.

80. *Id.* at 1529.

81. *Id.* at 1526–27.

82. CCIPS SEARCH-AND-SEIZURE MANUAL, *supra* note 73, at 65; Kerr, *supra* note 8, at 1026 (citing United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000)); Ohm, *supra* note 8, at 1527.

83. *See* CCIPS SEARCH-AND-SEIZURE MANUAL, *supra* note 73, at 65; Ohm, *supra* note 8, at 1527–28.

84. Ohm, *supra* note 8, at 1525.

85. *Id*.

86. *Id.* at 1525, 1535 (citing Freedman v. Am. Online, Inc., 412 F. Supp. 2d 174, 181–84 (D. Conn. 2005)). Additionally, although the Ninth Circuit held a showing of probable cause, instead of mere relevance, was necessary for government access to certain communications under the SCA, the United States Department of Justice has never petitioned the legislature to reverse this decision. *Id.* at 1536. Paul Ohm argues the United States Department of Justice's inaction indicates that the Ninth Circuit's enhanced standard matters little to law enforcement because "whenever the police have any suspicion in an online case, they have probable cause." *Id.* at 1541.

of stored e-mail surveillance, the importance of the probable cause justification standard is waning.

B. Warrantless Surveillance and the Unconstitutionality of the SCA

In an attempt to create a statutory version of the Fourth Amendment for computer networks, Congress enacted the SCA[87] in 1986 as part of the Electronic Communications Privacy Act.[88] The SCA governs the surveillance of stored e-mail content, delineating the procedural steps the government must take in order to access e-mail accounts and the communications contained therein. Enacted before e-mail became a central medium of communication, the SCA permits the government to compel disclosure of certain stored e-mails without a probable cause warrant.[89] This statutory framework is thus in disharmony with the Fourth Amendment's safeguards, safeguards which ensure the reasonableness of searches and seizures.

Many scholars questioning the constitutionality of the SCA have focused on this particular issue, recommending a warrant based on probable cause for all surveillance of stored e-mail communications.[90] Yet, since the Supreme Court addressed how and why wiretapping triggers Fourth Amendment protections in *Berger v. New York*[91] and *Katz v. United States*,[92] federal courts have generally avoided constitutional scrutiny of modern electronic-surveillance laws.[93] The Sixth Circuit's decision in *Warshak*,[94] however, indicates that courts are now willing to question the constitutionality of the SCA.

---

87. *See* United States v. Warshak, 631 F.3d 266, 335 (6th Cir. 2010) (Keith, J., concurring) ("The purpose of . . . the Stored Communications Act . . . is to maintain the boundaries between a citizen's reasonable expectation of privacy and crime prevention in light of quickly advancing technology."); United States v. Ahrndt, No. 08-468-KI, 2010 WL 373994, at *8 (D. Or. Jan. 28, 2010).

88. Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

89. 18 U.S.C. § 2703(b), (d) (2006 & Supp. III 2009) (authorizing compelled disclosure of contents originally maintained solely for purposes of "storage or computer processing" with a subpoena or court order).

90. *See, e.g.*, Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1436 (2004); Kerr, *supra* note 8, at 1043; Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1592 (2004); Solove, *supra* note 8, at 1299.

91. 388 U.S. 41 (1967).

92. 389 U.S. 347 (1967).

93. Freiwald, *supra* note 11, ¶ 2. *But see* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) ("[T]o the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional.").

94. 631 F.3d 266 (6th Cir. 2010).

Congress may provide additional statutory protections above the Fourth Amendment's safeguards when it chooses to do so,[95] but Congress cannot deny citizens the full panoply of protections the Fourth Amendment provides. Recognizing the constitutional pitfalls of the SCA and the attendant ramifications of the statute's inadequacies, some members of Congress have recently expressed the need to amend the SCA in order align searches and seizures of stored communications with the commands of the Fourth Amendment.[96] Twenty-five years after authoring the Electronic Communications Privacy Act, Senator Patrick Leahy introduced a bill on May 17, 2011 that uniformly requires the government to obtain a search warrant in order to access the contents of stored e-mail.[97]

Even if the scholars prevail, even if the SCA is amended to require the government to obtain a warrant based on probable cause to search and seize stored e-mail, and even if the courts follow the Sixth Circuit's lead, stored e-mails and files will be subject to unreasonable searches and seizures due to a lack of adequate Fourth Amendment protections. Obtaining a probable cause warrant is merely one component of the reasonableness inquiry. When a warrant lacks sufficient particularity, the subsequent search or seizure is considered warrantless and therefore presumptively unreasonable and unconstitutional.[98] It is the particularity requirement that provides additional protection and ensures the purpose of the probable cause requirement is not wholly aborted.[99] Probable cause and particularity work hand-in-hand: to establish probable cause for the issuance of a warrant, the government must demonstrate the described items are connected with the criminal activity under investigation and the items are to be found in the place to be searched.[100] The less precise the description of the things to be seized, the more likely it will be that one or both of those probabilities has not been established. [101]

To safeguard individual privacy, probable cause works in conjunction with particularity to keep the government out of constitutionally protected areas until it has reason to believe a specific crime has been

95. For example, Congress included procedural safeguards in the Wiretap Act derived from the particularity requirement above and beyond what the Fourth Amendment requires. *See* 18 U.S.C. § 2518(1)(c)–(f) (2006 & Supp. III 2009).
96. *See infra* note 97.
97. Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong., § 3 (2011).
98. *See* Groh v. Ramirez, 540 U.S. 551, 559–63 (2004).
99. Berger v. New York, 388 U.S. 41, 59 (1967).
100. *See* U.S. CONST. amend. IV.
101. 2 WAYNE LAFAVE, SEARCH AND SEIZURE § 4.6(a) (4th ed. 2009); *see also* Kerr, *supra* note 8, at 1045 ("The particularity requirement determines how far the government can search based on a particular factual predicate . . . the less the government can search, the harder it is for the government to abuse its powers to conduct wide-ranging searches . . . .").

or is being committed,[102] thereby prohibiting the "general, exploratory rummaging in a person's belongings."[103] By limiting the government's authorization to search only specific areas and seize only specific things for which probable cause exists, the particularity requirement ensures searches and seizures—electronic or otherwise—are tailored to their justifications.[104] Yet while much attention has been given to probable cause in the context of stored e-mail surveillance,[105] how the particularity requirement applies in that context is not well known or explored. A previously unanswered question therefore remains: how particular must warrants for stored e-mail communications be to satisfy the Fourth Amendment? The standards set forth below provide ample guidance to the courts and law enforcement to ensure warrants for stored e-mail communications are sufficiently particular to satisfy the Fourth Amendment.

IV. STORED E-MAIL PARTICULARITY IN PRACTICE

The manifest purpose of the particularity requirement is to prevent general warrants that authorize exploratory rummaging in a person's belongings—the government can only search specific places and seize specific things.[106] Thus, a search pursuant to a particularized warrant will not invade the privacy of the individual whose premises are to be searched and whose property is to be seized beyond what is necessary to achieve a valid law enforcement purpose.[107] In addition, requiring particularized warrants "assures the individual whose property is searched or seized of the lawful authority of the executing officer, his need to search, and the limits of his power to search."[108]

With the rise of the internet, the government has an increasing need to examine e-mails and files stored by ISPs. At the same time, the digital age heightens the privacy concerns implicated by broad searches and seizures of stored e-mail—as compared to the days of paper records.[109] A target e-mail account, in addition to containing e-mails relevant to an investigation, will undoubtedly contain e-mails

102. *Berger*, 388 U.S. at 59.

103. Andresen v. Maryland, 427 U.S. 463, 480 (1967) (quoting Coolidge v. New Hampshire, 403 U.S. 433 (1971)).

104. Maryland v. Garrison, 480 U.S. 79, 84 (1987).

105. *See, e.g.*, CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 21–47 (2007) (arguing for a "reconceptualization" of the Fourth Amendment's justification standards).

106. *Garrison*, 480 U.S. at 84; *Andresen*, 427 U.S. at 479.

107. United States v. Stefonek, 179 F.3d 1030, 1033 (7th Cir. 1999).

108. Groh v. Ramirez, 540 U.S. 551, 561 (quoting United States v. Chadwick, 433 U.S. 1, 9 (1977)).

109. United States v. Comprehensive Drug Testing, Inc. (*CDT II*), 621 F.3d 1162, 1177 (9th Cir. 2010).

and files the government has no probable cause to search and seize.[110] Greater vigilance on the part of judicial officers is thus required in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures.[111] Responsible judicial officers must take care to ensure stored e-mail searches and seizures occur in a manner that minimizes unwarranted intrusions upon privacy.[112] The purposes served by the Fourth Amendment provide guidance as to how the particularity requirement should be enforced—adequately protecting privacy interests in stored e-mail communications without unduly burdening government investigations.[113]

A. The Place to be Searched

The particularity requirement first mandates that warrants describe with particularity the place to be searched.[114] A description of the place to be searched is constitutionally reasonable if it is sufficiently particular to enable the executing law-enforcement agent to locate and identify the premises with reasonable effort, and if there is no reasonable probability that another premise might be mistakenly searched.[115]

In the digital realm, whether a description of a place to be searched is sufficiently particular is a complicated question because of the differences between the physical and digital worlds. As Orin Kerr notes, physicality limits scale in the physical world, and the particularity requirement is based on that scale.[116] The internet is different—a person likely has only one home in the physical world but can have multiple e-mail accounts maintained by multiple providers.[117] If e-

110. *See id.* at 1176 ("Seizure of . . . Google's email servers to look for a few incriminating messages could jeopardize the privacy of millions."); United States v. Cioffi, 668 F. Supp. 2d 385, 391 (E.D.N.Y. 2009).

111. *See CDT II*, 621 F.3d at 1177.

112. *See* Andresen v. Maryland, 417 U.S. 463, 482 n.11 (1967).

113. *See* LAFAVE, *supra* note 101, § 4.6(a) ("[O]ften a judgment as to the sufficiency of a description of items to be seized under a search warrant cannot be made by reference to earlier decisions . . . . Rather, such a judgment necessitates an evaluation of the description in question in terms of the purposes underlying the Fourth Amendment requirement of particularity.").

114. U.S. CONST. amend. IV.

115. United States v. Petti, 973 F.2d 1441, 1444 (9th Cir. 1992) (quoting United States v. Turner, 770 F.2d 1508, 1510 (9th Cir. 1985)); United States v. McCain, 677 F.2d 657, 660 (8th Cir. 1982); *cf.* United States v. Alexander, 761 F.2d 1294, 1300 (9th Cir. 1985) ("The particularity requirement inquires into the sufficiency of the description of the premises to be searched, and tests whether 'the officer with a search warrant can with reasonable effort ascertain and identify the place intended.'" (quoting Steele v. United States, 267 U.S. 498, 503 (1925))).

116. Kerr, *supra* note 8, at 1045.

117. *Id*. at 1045–46.

mails containing evidence of a crime are stored in one of several e-mail accounts belonging to a suspect, law enforcement might be unable to determine which account contains the sought-after e-mails, and law enforcement may thus be unable to search any one of the e-mail accounts.[118]

Kerr suggests that for online searches, the particularity requirement should be satisfied by identifying the individual under investigation rather than identifying a specific e-mail account.[119] Kerr comes to this conclusion by way of analogy to the statutory "roving wiretap" authority, which permits the government to wiretap any telephone line used by a person under investigation—rather than limit a wiretap to a specific telephone line.[120] Although the Federal Wiretap Act requires there be "a particular description of the nature and location of the facilities from which [information is sought] or the place where the communication is to be intercepted,"[121] such description is unnecessary as to the interception of wire or electronic communication if the suspect may try to thwart interception by changing facilities.[122] These roving wiretaps are therefore permitted if the government identifies "the person committing the offense and whose communications are to be intercepted."[123] Kerr argues these same principles should permit the government to search all e-mail accounts of an individual under investigation rather than require the government to specifically identify an e-mail account.[124]

Kerr's approach, however, is problematic for at least two reasons. To begin, it is true courts upheld the constitutionality of the roving wiretap statute despite challenges alleging insufficient adherence to the particularity requirement.[125] The statute has been held to provide sufficient particularization because only telephone facilities actually used by an identified speaker may be subject to surveillance,[126] and the Wiretap Act contains particularity safeguards that go beyond

118. *Id*. at 1046 (arguing that without knowledge of which e-mail account contains the sought-after e-mails, law enforcement may "lack probable cause to search any one account" and "[as] a result, every account will remain unsearched even if the police have probable cause to believe that the evidence" is in one of the accounts).
119. *Id*.
120. *Id*. at 1046–47 (citing 18 U.S.C. § 2518(11)(a) (2006 & Supp. III 2009)).
121. 18 U.S.C. § 2518(1)(b).
122. *Id*. § 2518(11).
123. *Id*.
124. Kerr, *supra* note 8, at 1047; *see* United States v. Lambert, 771 F.2d 83, 91 (6th Cir. 1985) (stating that particularization did not require judge issuing warrant for wiretap to approve the precise location in the house where each listening device would be placed).
125. *See, e.g.*, United States v. Gaytan, 74 F.3d 545 (5th Cir.1996); United States v. Bianco, 998 F.2d 1112 (2d Cir. 1993); United States v. Petti, 973 F.2d 1441, 1445 (9th Cir. 1992).
126. *Petti*, 973 F.2d at 1445.

what the Fourth Amendment requires.[127] The Wiretap Act's many safeguards concerning roving and fixed interceptions have thus been held to satisfy the Fourth Amendment requirement that "no greater invasion of privacy [occur] than [is] necessary to meet the legitimate needs of law enforcement."[128] However, the SCA does not contain the safeguards of the Wiretap Act, safeguards that eliminate the possibility of abuse or mistake and prevent wide-ranging exploratory searches.[129] Unless and until the SCA is amended to incorporate similar safeguards, Kerr's proposition falls short of satisfying the particularity requirement. Yet it is unlikely the SCA will be amended in this manner, as information acquired in real time has traditionally been afforded more protection than electronically stored information.[130]

In addition, permitting the government to scour every one of an individual's e-mail accounts would be akin to revenue officers in colonial days who scoured "suspected places" pursuant to a general warrant.[131] According to the United States Department of Justice, when probable cause to search relates to stored information, rather than to the storage device itself, the warrant should focus on the content of the relevant files rather than on the storage devices which might contain the files.[132] The particularity requirement was designed to ensure the government searches only *specific* places and that probable cause to search such places actually exists.[133] Granted, the Supreme Court has taken a flexible interpretation of the Fourth Amendment in order to keep pace with the technologically advancing society,[134] holding in *United States v. Karo*[135] that advance identification of the place

127. For example, the government is required to provide a statement as to "whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous" and must use standard minimization procedures to ensure that only conversations relating to a crime in which the speaker is a suspected participant are intercepted. *See* 18 U.S.C. §§ 2518(1)(c), (5).

128. *Petti*, 973 F.2d at 1445 (quoting Katz v. United States, 389 U.S. 357, 355–56 (1967)); *see also* United States v. Cox, 449 F.2d 679, 687 (10th Cir. 1971) (holding a warrant drafted in accordance with the requirements of the Wiretap Act will not "grant a roving commission or general warrant to seize any and all conversations").

129. *Cox*, 449 F. 2d at 687.

130. *See* JAMES G. CARR & PATRICIA L. BELLIA, THE LAW OF ELECTRONIC SURVEILLANCE § 1:14 (Thomson West ed., 2007); Freiwald, *supra* note 32, at 42–73 (comparing the procedures for online surveillance to those for wiretapping).

131. *See In re* United States of America's Application for a Search Warrant to Seize and Search Electronic Devices from Edward Cunnius, 770 F. Supp. 2d 1138 (W.D. Wash. 2011).

132. CCIPS SEARCH-AND-SEIZURE MANUAL, *supra* note 73, at 72.

133. *See* Steele v. United States, 267 U.S. 498, 501–02 (1925).

134. *See* Steagald v. United States, 451 U.S. 204, 218 n.10 (1981).

135. 468 U.S. 705 (1984).

to be searched was unnecessary in another context.[136] Yet in *Karo*, the government argued it was impossible to specify in advance the place to be searched because the location of the place was "precisely what [was] sought to be discovered through the search."[137]

In contrast, a description specifically identifying the e-mail account should be included in a warrant if the government uncovers an e-mail address—or other information that can be traced to a particular e-mail account—containing the targeted communications.[138] If the government does not know and cannot obtain this information, Kerr's approach regarding particularity of the *place to be searched* seems promising. However, as to the Fourth Amendment's requirement that warrants must also particularly describe the *things to be seized*, Kerr's solution falls short.

B. The Things to be Seized

The second part of the particularity requirement commands that warrants particularly describe the things to be seized, thereby preventing the seizure of one thing under a warrant that describes another.[139] According to the Supreme Court, "[a]s to what is to be taken, nothing is left to the discretion of the officer executing the warrant."[140] Because surveillance of stored e-mail communications involves privacy intrusions that are broad in scope, courts authorizing such surveillance have a responsibility to issue warrants that afford "similar protections to those [protections] that are present in the use of conventional warrants authorizing the seizure of tangible evidence."[141]

Drawing from established principles of particularity in both the physical and digital realm, this Section sets forth the rules that govern the constitutional sufficiency of a warrant which describes stored e-mails and files to be seized. Central to these rules is the basic tenet that the Fourth Amendment requires the government to describe the stored e-mails and files to be seized with as much detail as its knowledge and the circumstances allow.[142] The proposed parameters of particularity emphasize a warrant authorizing the government to seize stored e-mails should focus on e-mail content. To begin, such a warrant should identify the individual under investigation and the

136. *Id*. at 718.
137. *Id.*
138. *See* United States v. Donovan, 429 U.S. 413, 427 n.15 (1977) ("The Fourth Amendment requires specification of 'the place to be searched . . . .' In the wiretap context, [that requirement is] satisfied by identification of the telephone line to be tapped . . . .").
139. Marron v. United States, 275 U.S. 192, 196 (1927).
140. *Id*.
141. *See* Berger v. New York, 388 U.S. 41, 57 (1967).
142. *See infra* note 159 and accompanying text.

other parties to the e-mail communication, if known. Furthermore, the government should seize only those stored e-mails and files sent or received during the time period the evidence suggests the criminal activity occurred. Lastly, warrants should identify the specific crime to which the stored e-mails or files relate. These safeguards ensure the authorization to seize stored e-mail communications is carefully circumscribed so as to prevent unauthorized invasions of privacy.[143]

1. Principles of Describing the Things to be Seized

Particularly describing the things to be seized has two distinct elements.[144] First, the description of the things to be seized must be limited to the scope of the probable cause established in the warrant.[145] A warrant's description of the stored e-mails and files should be rendered defective if it is broader than the probable cause upon which the warrant is based.[146] Courts will consider whether probable cause exists to seize all items of a particular category described in the warrant to determine whether a description of the items is overbroad.[147] This "consideration encapsulates the overarching Fourth Amendment principle that police must have probable cause to search and seize all the items of a particular type described in the warrant."[148] Probable cause to believe that *some* incriminating e-mails will be present in an

143. *See Berger*, 388 U.S. at 57 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

144. *See* United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999).

145. *See In re* Grand Jury Investigation Concerning Solid State Devices, Inc., 130 F.3d 853, 857 (9th Cir. 1997).

146. LAFAVE, *supra* note 101, § 4.6(a) ("[A]n otherwise unobjectionable description of the objects to be seized is defective if it is broader than can be justified by the probable cause upon which the warrant is based."); *see also* Millender v. Cnty. of L.A., 620 F.3d 1016, 1025 (9th Cir. 2010) (stating probable cause to search for documents pertaining to "certain aspects of an operation" cannot justify the seizure of all documents in an office); United States v. Bentley, 825 F.2d 1104, 1110 (7th Cir. 1987) ("When the probable cause covers fewer documents in a system of files, the warrant must . . . tell the officers how to separate the documents to be seized from others."); Rickert v. Sweeney, 813 F.2d 907, 909 (8th Cir. 1987) ("Although probable cause existed to search the records of one particular project, the warrant failed to so limit the search."); United States v. Spilotro, 800 F.2d 959, 967 (9th Cir. 1986) (providing a list of criminal statutes in warrant that went beyond probable cause in affidavit); Voss v. Bergsgaard, 774 F.2d 402, 408 (10th Cir. 1985) (Logan, J., concurring) ("The breadth of a warrant must be justified by the breadth of the probable cause."); *cf.* VonderAhe v. Howland, 508 F.2d 364, 369 (9th Cir. 1974) ("[A]lthough there may have been 'probable cause' to search for and seize [records of a certain type and date] there was no probable cause shown for a seizure of all the . . . books and records, or . . . personal and private papers.").

147. *Millender*, 620 F.3d at 1025.

148. *Id.* at 1030; *see also* United States v. SDI Future Health, Inc., 568 F.3d 684, 702–03 (9th Cir. 2009); *In re* Grand Jury Subpoenas Dated Dec. 10, 1987, 926 F.2d 847, 857 (9th Cir. 1991); *VonderAhe*, 508 F.2d at 369–70.

e-mail account does not necessarily mean there is probable cause to believe there will be more of the same.[149] Courts will not mechanically reason "some implies more;" rather, pre-warrant investigations, as described in affidavits presented to a magistrate judge, must establish probable cause that more e-mails are contained in the account that provide evidence of the crime under investigation.[150] "The premise here is that *any* intrusion in the way of search or seizure is an evil, so that no intrusion at all is justified without a careful prior determination of necessity."[151] This prevents fishing expeditions—limiting searches to the suspected criminal activity.[152]

For example, imagine a woman named Sheila reports to law enforcement agents that her ex-husband Brian has been sending her harassing e-mails. Sheila cannot produce the e-mails, however, because Brian hacked her e-mail account, deleted all of her e-mails, and changed her password, consequently preventing her from accessing her account. If the government establishes probable cause to seize the harassing e-mails from Brian's e-mail account, but has no reason to believe the other e-mails in his account contain incriminating information, there is no probable cause to justify seizing Brian's non-harassing e-mails.[153]

Second, a warrant must describe the things to be seized with sufficiently precise language so that it informs the officers how to separate the items that are properly subject to seizure from those that are irrelevant.[154] A warrant's description of the e-mails to be seized must provide objective guidance to government agents conducting the

149. *See* United States v. Weber, 923 F.2d 1338, 1344 (9th Cir. 1990) (Stewart, J., plurality).

150. *Id*. (citing United States v. Hillyard, 677 F.2d 1336, 1339–40 (9th Cir. 1982)).

151. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).

152. *See* Groh v. Ramirez, 540 U.S. 551, 560–61 (2004).

153. *See SDI Future Health, Inc*., 568 F.3d at 704 (holding a portion of a search warrant authorizing the search for "[d]ocuments relating to non-privileged internal memoranda and E-mail" was invalid when the government's interest was limited to communications related to sleep studies); *Weber*, 923 F.2d at 1343 (citing *VonderAhe*, 508 F.2d at 370).

154. *See* Marron v. United States, 275 U.S. 192, 296 (1927) ("As to what is to be taken, nothing is left to the discretion of the officer executing the warrant."); Davis v. Gracey, 111 F.3d 1472, 1478 (10th Cir. 1997); Williams v. Kunze, 806 F.2d 594, 598 (5th Cir. 1986) ("The items to be seized must be described with sufficient particularity such that the executing officer is left with no discretion to decide what may be seized.").

search[155] so they may distinguish between those e-mails they can seize and those they cannot.[156]

When the government has probable cause during an online investigation, it generally has an arsenal of information at its fingertips.[157] Evidence of a crime collected during an investigation often reveals critical information such as the date of the crime's commission, the specific times the crime occurred, the identities of the perpetrators, and the subject matter to which the crime pertains.[158] If there is indeed probable cause to believe e-mails stored in an account are contraband, or contain contraband such as fruits or instrumentalities of the crime, the government can likely seize such information and use it to narrow the universe of e-mail communications it seeks to obtain.

Courts have routinely deemed warrants insufficiently particular if information known or available to the government is not used to narrow the description of the items to be seized. [159] Thus, warrants have

155. *See* Lo-Ji Sales, Inc. v. New York, 442 U.S. 319, 325 (1979); Stanford v. Texas, 379 U.S. 476, 485 (1965); United States v. Rosa, 626 F.3d 56, 62 (2nd Cir. 2010) (holding a warrant failed the particularity requirement because it "directed officers to seize and search certain electronic devices, but provided them with no guidance as to the type of evidence sought"); United States v. Williams, 592 F.3d 511, 519 (4th Cir. 2010) (citing Andresen v. Maryland, 427 U.S. 463, 480–82 (1976)); United States v. Adjani, 452 F.3d 1140, 1148 (9th Cir. 2006) (citing United States v. Spilotro, 800 F.2d 959, 963 (9th Cir. 1986)); United States v. Biasucci, 786 F.2d 504, 510 (2nd Cir. 1986) ("[T]he Constitution requires particularization in the warrant, i.e., the warrant must describe . . . the information sought."); *see also* 18 U.S.C. § 2518(1)(b) (2006 & Supp. III 2009) (imposing the same requirements to obtain a wiretap order); United States v. Cioffi, 668 F. Supp. 2d 385, 392 (E.D.N.Y. 2009) (holding warrant violated the particularity requirement where it authorized the search of all e-mails in a defendant's e-mail account but did not limit the search to e-mails related to the alleged crime and did not incorporate by reference the affidavit containing the description of the alleged crime and the associated use of the target e-mail account).

156. *See Marron*, 275 U.S. at 196 ("As to what is to be taken, nothing is left to the discretion of the officer executing the warrant."); *Gracey*, 111 F.3d at 1478; United States v. Hayes, 794 F.2d 1348, 1356 (9th Cir. 1986).

157. *See supra* section II.A.

158. *See, e.g.*, United States v. Burdulis, No. 10-40003-FDS, 2011 WL 1898941, at *6 (D. Mass. May 19, 2011) (providing that police conducting online investigation obtained file names, dates, times, and content of e-mails and pictures).

159. *See, e.g.*, United States v. Leary, 846 F.2d 592, 600 (10th Cir. 1988) ("[T]he fourth amendment [sic] requires that the government describe the items to be seized with as much specificity as the government's knowledge and circumstances allow, and warrants are conclusively invalidated by their substantial failure to specify as nearly as possible the distinguishing characteristics of the goods to be seized."); United States v. Fuccillo, 808 F.2d 173, 176 (1st Cir. 1987) ("In light of the information available to the agents which could have served to narrow the scope of the warrant and protect the defendants' personal rights, the warrant was inadequate." (quoting United States v. Klein, 565 F.2d 183, 190 (1st Cir. 1977)) (internal quotations omitted)), United States v. Cook, 657 F.2d 730, 733 (5th Cir. Unit A Sept. 1981) ("Failure to employ the specificity available will invalidate a general description in a warrant."); VonderAhe v. Howland, 508 F.2d 364, 370

been invalidated when the government had information that would have particularized the description of items to be seized but failed to include such information in the warrant.[160] Requiring the government to use the information it has acquired during an investigation to specifically describe targeted, stored e-mails limits the possibility that the government will seize communications beyond what is justified by the established probable cause.[161] Additionally, failure to describe the items to be seized with as much particularity as the circumstances reasonably allow offends the Fourth Amendment because there is no assurance the permitted invasions of privacy and property are no more than absolutely necessary.[162]

Considered together, the two elements of particularly describing the things to be seized prevent government agents from executing the free-ranging "general warrant" the framers intended to prohibit.[163] The elements instead require agents to conduct narrow seizures that minimize unwarranted intrusions upon privacy.[164] Both Congress and courts have recognized the need for particularity is especially great when electronic surveillance involves broadly scoped intrusions on privacy.[165] Concerned with the threats that electronic surveillance poses to individual privacy and liberty, courts have required such surveillance to be "carefully circumscribed" so as to prevent unauthorized invasions of privacy.[166]

The privacy invasions that result from stored e-mail surveillance are broad indeed. The government frequently exercises its power to access the contents of stored e-mails without limiting the scope of the communications sought, as demonstrated by the introductory hypothetical,[167] based on the facts of *United States v. Warshak*.[168] In *Warshak*, the government acquired approximately 27,000 of Steven Warshak's stored e-mails which contained his entire business and per-

(9th Cir. 1974) ("Upon the information available to it, the government knew exactly what it needed and wanted . . . . There was no necessity for a massive reexamination of all records.").

160. *See supra* note 159 and accompanying text.

161. *See* LAFAVE, *supra* note 101, § 4.6(a).

162. *See* Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971); United States v. Cardwell, 680 F.2d 75, 78 (9th Cir. 1982); United States v. Klein, 565 F.2d 183, 186 (1st Cir. 1977); United States v. Marti, 421 F.2d 1263, 1268 (2nd Cir. 1970).

163. *See* Maryland v. Garrison, 480 U.S. 79, 84 (1987).

164. Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1967).

165. Berger v. New York, 388 U.S. 41, 56 (1967) ("The 'indiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments,' and imposes 'a heavier responsibility on this Court in its supervision of the fairness of procedures . . . .'" (quoting Osborn v. United States, 385 U.S. 323, 329 n.7 (1966))).

166. *Id.* at 55, 58.

167. *See supra* Part I.

168. 631 F.3d 266 (6th Cir. 2010).

sonal life,[169] but the government did not narrow its acquisition based on need.[170] E-mail accounts are much like computer hard drives because "[i]ndividuals may store personal letters, e-mails, financial information, passwords, family photos, and countless other items of a personal nature in electronic form" accounts which are "capable of holding a universe of private information."[171] In *United States v. Otero*,[172] the Tenth Circuit noted the ability of computers "to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement that much more important."[173]

2. Particularity Parameters

In the face of advancing surveillance techniques, it is not novel to establish rules that pertain to descriptions of places to be searched and things to be seized in order to satisfy the particularity requirement. In *Berger*, the Supreme Court held the "failure to describe with particularity the conversations sought gives the officer a roving commission to 'seize' any and all conversations" in violation Fourth Amendment.[174] The Court held the lack of particularity gave the government too much discretion when executing wiretap searches and seizures.[175] To prevent such violations, the Wiretap Act requires the government to describe the types of conversations sought before it can utilize a wiretap.[176] This procedural protection has been extended to the government's use of silent video surveillance because such surveillance exhibits the same constitutional infirmities as wiretapping.[177] Seven federal appellate courts have held the government must first

169. *Id*. at 281–82.

170. Freiwald, *supra* note 11, ¶ 68 (stating the defendant in *Warshak* claimed the government obtained thousands of emails "without any particularization or limitation as to time frame, parties to the communication, or the subject matter of the communication").

171. *See* United States v. Mitchell, 565 F.3d 1347, 1351–52 (11th Cir. 2009).

172. 563 F.3d 1127 (10th Cir. 2009).

173. *Id*. at 1132; *see In re* United States of America's Application for a Search Warrant to Seize and Search Electronic Devices from Edward Cunnius, 770 F. Supp. 2d 1138, 1144 (W.D. Wash. 2011) ("There are just too many secrets on people's computers, most legal, some embarrassing, and some potentially tragic in their implications, for loose liberality in allowing search warrants.").

174. Berger v. New York, 388 U.S. 41, 59 (1967).

175. *Id*.; *see* Lo-Ji Sales, Inc. v. New York, 442 U.S. 319, 325 (1979); United States v. Williams, 592 F.3d 511, 519 (4th Cir. 2010) (citing Andresen v. New York, 427 U.S. 463, 480–82 (1976); Stanford v. Texas, 379 U.S. 476, 485 (1965)).

176. 18 U.S.C. § 2518(1)(b) (2006 & Supp. III 2009).

177. *See* Freiwald, *supra* note 32, at 79–80.

describe with particularity the activity sought to be videotaped before a warrant authorizing such surveillance is granted.[178]

The same principle driving this procedural protection in context of wiretaps and silent videos applies to stored e-mail surveillance, and the intrusiveness of stored e-mail surveillance commands the same restriction.[179] In *Berger*, the Court analogized eavesdropping over a two-month period to a "series of intrusions, searches, and seizures [based on one] showing of probable cause."[180] Likewise, when the government seizes the entirety of an individual's e-mail account, it obtains a continuous record of a person's private affairs with a single authorization.[181] As such, the scope of an e-mail seizure must be constrained by content.[182] While the government may not be required to seek court approval of each and every precise e-mail to be seized,[183] warrants should describe the content of targeted e-mails and files with as much detail as possible, rather than focus on the e-mail account which may happen to contain them.[184] Such specific descriptions are necessary to avoid the type of indiscriminate rummaging the Fourth Amendment was intended to prohibit.[185] Therefore, warrants for stored e-mails should fail for want of particularity if the e-mails to be seized could be narrowed by certain parameters—discussed below—when such information is known or ascertainable by the government.

178. *See* Freiwald, *supra* note 11, ¶ 54 (citing United States v. Koyomejian, 970 F.2d 536, 542 (9th Cir. 2002)).

179. *Id.* ¶¶ 62–70; *see also supra* Part II (discussing the analogy between wiretaps and e-mail surveillance).

180. *Berger*, 388 U.S. at 59.

181. Freiwald, *supra* note 11, ¶ 70.

182. *See* United States v. Stabile, 633 F.3d 219, 238–39 (3d Cir. 2011) (quoting United States v. Burgess, 576 F.3d 1078, 1093 (10th Cir. 2009)); *see also* United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009) ("[W]arrants for computer searches must *affirmatively limit* the search to evidence of specific federal crimes or specific types of material." (quoting United States v. Riccardi, 405 F.3d 852, 862 (10th Cir. 2005))).

183. *See* United States v. Silberman, 732 F. Supp. 1057, 1061 n.8 (S.D. Cal. 1990) ("[A] strict interpretation of the particularity requirement as to things seized would require court approval of each and every conversation that would be monitored prior to the actual monitoring. This is clearly not required under the Fourth Amendment.").

184. *See* United States v. Vilar, No. S305CR621KMK, 2007 WL 1075041, at *36 (S.D.N.Y. Apr. 4, 2007) ("[U]nderlying information must be identified with particularity and its seizure independently supported by probable cause."); CCIPS SEARCH-AND-SEIZURE MANUAL, *supra* note 73, at 70, 72 (citing United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999)).

185. *See Berger*, 388 U.S. at 59; *see also* United States v. Allen, 625 F.3d 830, 835 (5th Cir. 2010) ("A general order to explore and rummage through a person's belongings is not permitted."); *Riccardi*, 405 F.3d at 862–63 (providing that a search must not be a wide-ranging exploration (quoting Maryland v. Garrison, 480 U.S. 79, 84 (1987))).

i. Specifying Identity

Warrants for stored e-mails should identify the person under investigation and the other suspected, involved individuals or entities whose communications are sought, if such identities are known to the government at the time the warrant is issued.[186] For instance, when the government applies for a wiretap order, the Wiretap Act requires the application for authorization state "the identity of the person, if known, committing the offense and whose communications are to be intercepted"[187] and that the wiretap order "shall . . . specify the identity of the person, if known, whose communications are to be intercepted." [188]

Interpreting the former statutory requirement, the Supreme Court noted in *United States v. Donovan*[189] that Congress included the identification requirement in response to *Berger* and *Katz*—the requirement was intended to "reflect . . . the constitutional command of particularization."[190] The Court held "a wiretap application must name an individual if the [g]overnment has probable cause to believe that the individual is engaged in the criminal activity under investigation and expects to intercept the individual's conversations over the target telephone."[191]

186. *See* United States v. Hanna, Nos. 09–1425, 09–2086, 2011 WL 3524292, at *11 (6th Cir. Aug. 12, 2011) (holding warrants for stored e-mails limited to searches of the person and company under investigation were sufficiently particular); United States v. Kow, 58 F.3d 423, 427 (9th Cir. 1995) (holding warrant insufficiently particular in part because "the government did not contain the scope of the warrant by reference to limiting descriptions in the affidavit such as HK Video's tax identification number, HK Video's account number at the Bank of Trade, or the names of the foreign companies allegedly receiving the proceeds of the defendants' profit-skimming"); *In re* Grand Jury Subpoenas Dated Dec. 10, 1987, 926 F.2d 847, 857 (9th Cir. 1991) (holding warrants contained a list of a variety of documents as objects of the search but the list was qualified by the requirement that the document seized be "in the name of or have reference to" the target of the investigation or one of the twenty-one persons or entities linked to the target through the investigation); United States v. Mesa-Rincon, 911 F.2d 1433, 1440 (10th Cir. 1990); Nat'l City Trading Corp. v. United States, 635 F.2d 1020, 1021 (2d Cir. 1980) (finding warrant was limited to "property of National City Trading Corp. and persons associated with it"); *see also* Kerr, *supra* note 8, at 1045–47 (arguing the particularity requirement should restrict an online investigation to a specifically named person); *cf.* United States v. Vogel, No. 4:08-CR-224(1), 2010 WL 2268237, at *7 (E.D. Tex. May 25, 2010) (holding warrant did not limit evidence seized to communications between defendant, co-conspirators, and other persons relevant to the investigation because government was not fully aware of all the parties involved in a large conspiracy).

187. 18 U.S.C. § 2518(1)(b)(iv) (2006 & Supp. III 2009).

188. *Id*. § 2518(4)(a).

189. 429 U.S. 413 (1977).

190. *Id.* at 426–27.

191. *Id*. at 428.

It is worth noting that it may not be constitutionally fatal if a warrant does not specifically name the identities of all parties connected to the targeted e-mail communications.[192] In the wiretap context, for example, the government is not required to specify each individual whose conversations may be intercepted in the wiretap. Where the government investigates numerous members of an extensive or complex criminal scheme, the government may not be able to identify each person who will use—for criminal purposes—the particular telephone under surveillance.[193] As such, the government need only identify all persons for whom such probable cause exists.[194] Thus, if the government has probable cause to believe *specific* individuals are engaged in the criminal activity under investigation and expects to seize stored e-mails from their e-mail accounts, the warrant should include their identities.[195]

The Supreme Court speculated that Congress codified the Wiretap Act's identification requirement after concluding the particularity requirement demands the naming of all suspects in a wiretap application.[196] If the particularity requirement commands the identification of all persons for whom such probable cause exists in the wiretap context, so too should a warrant for the contents of stored e-mails name all such persons. Yet the Supreme Court seems to disagree with Congress's interpretation of the particularity requirement. According to the Supreme Court:

> The Fourth Amendment requires specification of "the place to be searched, and the persons or things to be seized." In the wiretap context, those requirements are satisfied by identification of the telephone line to be tapped and the particular conversations to be seized. It is not a constitutional requirement that all those likely to be overheard engaging in incriminating conversations be named. Specification of this sort "identif[ies] the person whose constitutionally protected area is to be invaded rather than 'particularly describing' the communications, conversations, or discussions to be seized."[197]

Extending the Court's interpretation to stored e-mail surveillance, a warrant should identify the e-mail account—akin to a telephone line—as the place to be searched and the written, e-mail conversations—akin to telephone conversations—as the things to be seized.[198]

192. *Id*.
193. United States v. Yannotti, 541 F.3d 112, 124 (2nd Cir. 2008).
194. *Donovan*, 429 U.S. at 428.
195. *See id*.; United States v. Leary, 846 F.2d 592, 604 (10th Cir. 1988) ("The warrant could have been limited to documents related to . . . the companies suspected of participating in the illegal export."); *see also* United States v. Buck, 813 F.2d 588, 590 (2nd Cir. 1987) (holding warrant sufficiently particular if law enforcement acquires all the descriptive facts which a reasonable investigation could be expected to cover and insures that all those facts are included in the warrant).
196. *See Donovan*, 429 U.S. at 427.
197. *Id*. at 427 n.15 (quoting Berger v. New York, 388 U.S. 41, 59 (1967)).
198. *See id*.

Requiring warrants to identify the e-mail account to be searched would, in many cases, have the same practical effect as if the individual were referenced by name. Often, albeit not always, an e-mail account is tied to a single individual. As previously discussed, when the government learns the e-mail address of an individual under investigation, it can subpoena the ISP associated with that address and obtain the individual's name and home address.[199] It would not, therefore, be unduly burdensome to require the government to identify the individual under investigation. Nor would the failure to do so render a stored e-mail warrant invalid. However, combined with the parameters discussed below, requiring warrants to identify—at a minimum—the target e-mail account would prevent government agents from exercising unfettered discretion and from seizing stored e-mails for which there is insufficient justification.[200]

ii. Establishing a Time Frame

Depending on the server, the ISPs terms of use, and the account holder's preferences or actions, e-mails and files are stored by ISPs for varying lengths of time.[201] With a warrant for e-mails and files stored in an account, the government can acquire a continuous record of the targeted communications in a single shot.[202] This creates a danger the government, while examining certain stored emails or files, will also examine a great many other stored communications in order to exclude the possibility that the sought-after information is concealed therein.[203]

When investigating agents know the evidence in support of probable cause revolves around a specific time frame, "the authorization to search for evidence irrelevant to that time frame could well be described as 'rummaging.'"[204] Although the government may be unable to exactly describe the stored contents sought, its failure to limit broad descriptions of e-mails and files by the relevant time period will render a warrant overbroad when the government knows or can ascertain relevant dates.[205] Accordingly, if the government knows when

199. *See supra* note 82 and accompanying text.
200. *Cf.* United States v. Kahn, 415 U.S. 143, 154 (1974) (holding a wiretap order containing a particular description of the type of communications sought to be intercepted, a statement of the particular offense to which the communications relate, and requiring surveillance minimization was not a "virtual warrant" and did not give federal agents unfettered discretion).
201. *See* DEUTCHMAN & MORGAN, *supra* note 37, at 10.
202. Freiwald, *supra* note 11, ¶ 70.
203. United States v. Comprehensive Drug Testing, Inc. (*CDT II*), 621 F.3d 1162, 1176 (9th Cir. 2010).
204. *E.g.*, United States v. Abboud, 438 F.3d 554, 576 (6th Cir. 2006).
205. *Cf.* United States v. Hanna, Nos. 09-1425, 09-2086, 2011 WL 3524292, at *11 (6th Cir. Aug. 12, 2011) (holding warrants for stored e-mails were not overbroad

the criminal activity under investigation occurred, a warrant should authorize the seizure of only those stored e-mails sent and received during the time frame the crimes were allegedly committed.[206]

For context, remember the example of Sheila, who filed a complaint alleging her ex-husband, Brian, was sending harassing e-mails. If Sheila informs investigating agents that Brian sent her harassing e-mails between January and February 2011, the warrant should authorize the agents to seize only those e-mails sent from Brian to Sheila between January and February 2011. In such a case, failure to limit the warrant to the known time frame would render the warrant insufficiently particular—providing for the seizure of stored e-mails and files for which no probable cause was established.[207]

iii. Specifying the Offense

The particularity requirement necessitates that an e-mail seizure be designed to target e-mails or files that could reasonably be believed to have some connection to the alleged crime under investigation.[208] While it may sometimes be difficult for the government to identify the exact communications sought,[209] it cannot have carte blanche to seize whatever it chooses—only evidence of the criminal activity under investigation may be seized.[210] As is the rule in other contexts, the gov-

---

where they limited searches to the "time period that the evidence suggested the activity occurred—between 2001 and 2004"); United States v. Lazar, 604 F.3d 230, 239 (6th Cir. 2010) ("Failure to limit broad descriptive terms by relevant dates, when such dates are available to the police, will render a warrant overbroad."); *Abboud*, 438 F.3d at 576 (holding a warrant was invalid as overbroad where it authorized search for records from January 1996 to May 2002, but where there was only probable cause shown for a three–month period in 1999); United States v. Kow, 58 F.3d 423, 427 (9th Cir. 1995) (holding a warrant was insufficiently particular when "[t]he government did not limit the scope of the seizure to a time frame within which the suspected criminal activity took place" and when such time frame was known by law enforcement); United States v. Leary, 846 F.2d 592, 604 (10th Cir. 1988) ("The warrant could have been limited to documents related to . . . a specific period of time coincident to the suspect transaction."); United States v. Spilotro, 800 F.2d 959, 965 (9th Cir. 1982) ("[T]he government's investigation centered upon specific business records, enabling it to refine the scope of the warrant by reference to particular criminal episodes, time periods, and subject matter. Because the government knew 'exactly what it needed and wanted,' . . . there was no need for so broad a warrant." (citing United States v. Cardwell, 680 F.2d 75, 78 (9th Cir. 1982))); United States v. Abrams, 615 F.2d 541, 542–43 (1st Cir. 1980) (finding a failure to restrict dates of target documents violated the particularity requirement).

206. *See supra* notes 204–05 and accompanying text.

207. *See supra* notes 204–05 and accompanying text.

208. United States v. Warshak, 490 F.3d 455, 476 n.8 (6th Cir. 2007).

209. *See* United States v. Vanichromanee, 742 F.2d 340, 347 (7th Cir. 1984) (holding a warrant that only authorized seizure of writings related to the conspiracy to import heroin did not need to specify precise documents).

210. United States v. Hayes, 794 F.2d 1348, 1356 (9th Cir. 1986).

ernment should seize only those e-mails and files related to the crime under investigation.[211]

Requiring warrants to specify the crime under investigation serves a distinct objective of the warrant requirement: that searches deemed necessary are as limited as possible.[212] *Berger* held the particularity requirement mandates such detail in the context of wiretapping.[213] As a result, the Wiretap Act requires that a warrant to intercept communications contain "a statement of the particular offense to which it relates."[214] This provision is a "safeguard against electronic surveillance that picks up more information than is strictly necessary and consequently violates the Fourth Amendment's requirement of particular description."[215] For this reason, courts have extended this requirement to the government's use of silent video surveillance.[216]

In many circumstances, the seizure of all e-mails contained in an individual's account will uncover more information than strictly necessary to further an investigation. Identifying the specific crime to which the sought-after stored e-mails and files relate enables law enforcement to reasonably ascertain and identify those communications that are within the scope of the probable cause established.[217] In contrast, the seizure of all electronically stored evidence of any crime in any jurisdiction allows precisely the kind of rummaging through a person's e-mail account, in search of evidence of even previously unsuspected crimes, that the Fourth Amendment proscribes.[218] For this reason, courts have required warrants to contain "sufficiently particularized language," creating "a nexus" with the crime to be investigated and have invalidated warrants as overly broad for failing to do so.[219] As such, warrants for stored e-mails and files should provide details as to the particular offense that has been committed, is being committed, or is about to be committed, to which the sought-after communications relate.[220]

---

211. *Id*. (citing United States v. Whitten, 706 F.2d 1000, 1009 (9th Cir. 1983)).
212. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).
213. Berger v. New York, 388 U.S. 41 (1967).
214. 18 U.S.C. § 2518(4)(c) (2006 & Supp. III 2009).
215. United States v. Torres, 751 F.2d 875, 883 (7th Cir. 1984).
216. *See* Freiwald, *supra* note 11, ¶ 54 (citing United States v. Koyomejian, 970 F.2d 536, 542 (9th Cir. 1992)).
217. United States v. Cook, 657 F.2d 730, 733 (5th Cir. Unit A Sep. 1981).
218. *See* Cassady v. Goering, 567 F.3d 628, 635 (10th Cir. 2009) (quoting Voss v. Gergsgaard, 774 F.2d 402, 405 (10th Cir. 1985)).
219. United States v. Burgess, 576 F.3d 1078, 1091 (10th Cir. 2009); United States v. Hall, 142 F.3d 988, 996–97 (7th Cir. 1998) ("[T]he search warrants were written with sufficient particularity because the items listed on the warrants were qualified by phrases that emphasized that the items sought were those related to child pornography.").
220. *See, e.g.*, United States v. Rosa, 626 F.3d 56, 62 (2nd Cir. 2010) ("The warrant was defective in failing to link the items to be searched and seized to the sus-

Even if the government asserts a violation of a particular federal statute, this alone may not be a sufficient limitation on a seizure of stored e-mails or files.[221] While some federal statutes may be narrow enough to meet the Fourth Amendment's requirement, courts have held the mere reference to a statute that covers a broad range of criminal activity does not sufficiently limit the scope of a seizure.[222] For example, in *Voss v. Bergsgaard*, [223] the government established probable cause of a tax-fraud scheme.[224] However, the warrant was not restricted to evidence relating to tax fraud, consequently permitting the government to seize books and records that were "evidence of violations of Title 18, United States Code, Section 371," a statute that prohibits conspiracies to violate any other federal statute.[225] The court held "even if the reference to [§] 371 is construed as a limitation, it does not constitute a constitutionally adequate particularization of the items to be seized" because that statute itself is extremely broad in scope and therefore placed no real limitation on the warrant.[226]

The court in *Voss* noted the dangers inherent in allowing references to broad criminal statutes to serve as sufficient limitations that satisfy the particularity requirement.[227] The warrant allowed for "the seizure of all books, records, or documents relating to customer accounts" concerning the general federal conspiracy statute.[228] The court noted:

> [E]vidence in a customer's file indicating a conspiracy on that customer's part to import marijuana, even if unrelated to tax fraud, is within the scope of the warrant and may lawfully be seized. This, despite the fact that the government presented no evidence even suggesting probable cause for believing a drug crime had been committed.[229]

---

pected criminal activity . . . and thereby lacked meaningful parameters on an otherwise limitless search of Rosa's electronic media."); United States v. Kow, 58 F.3d 423, 427 (9th Cir. 1995) ("The government could have made the warrant more particular. Most obviously, the warrant could have specified the suspected criminal conduct."); United States v. Biasucci, 786 F.2d 504, 510 (2nd Cir. 1986) ("[T]he Constitution requires particularization in the warrant, i.e., the warrant must describe . . . the crime that has been, is being, or is about to be committed.").

221. *See* United States v. Leary, 846 F.2d 592, 602 (10th Cir. 1988); United States v. Cardwell, 680 F.2d 75, 77 (9th Cir. 1982) ("The only limitation on the search and seizure of appellants' business papers was the requirement that they be the instrumentality or evidence of violation of the general tax evasion statute. . . . That is not enough."); United States v. Abrams, 615 F.2d 541, 542–43 (1st Cir. 1980) (holding a warrant that was limited only by reference to records and a federal fraud statute was overbroad).
222. *Leary*, 846 F.2d at 601.
223. 774 F.2d 402 (10th Cir. 1985).
224. *Id*. at 404–05.
225. *Id*. at 405.
226. *Id*. (citing United States v. Roche, 614 F.2d 6, 8 (1st Cir. 1980)).
227. *Id.*
228. *Id*.
229. *Id*.

This same rationale should be applied to warrants for stored e-mails and files. For example, a warrant for stored e-mails evidencing violations of the mail-fraud statute, which makes illegal *all* frauds that utilize the mail,[230] would be insufficiently particular without limiting the seizure to specific transactions or time periods.[231]

Again, it may be difficult for the government to identify exactly which e-mails stored in an account are evidence of the crime under investigation. Thus there may be situations where seizure of all electronically stored e-mails or files may be necessary. Yet for such language to pass constitutional muster, the government should specify that all of the e-mails and files relate to a narrow, criminal statute, thereby ensuring the subsequent seizure does not extend beyond the probable cause established. In contrast, reference to a federal statute encompassing a broad range of criminal activity will be permissible only when a statutory reference is limited by the specific descriptions of the e-mails sought.[232]

3. Confronting the Plain Text Argument

The proposed particularity standards will help ensure that investigating agents clearly understand what it is they are seeking to seize, consequently enabling them to conduct stored-e-mail-surveillance in a way that avoids searching and seizing e-mails and files of types not identified.[233] However, in *United States v. Grubbs*,[234] the Supreme Court interpreted the particularity requirement narrowly, adding to the list of opinions rejecting efforts to expand its scope.[235] The Court held the Fourth Amendment "does not set forth some general 'particu-

230. 18 U.S.C. § 1341 (2006 & Supp. III 2009).

231. *See Roche*, 614 F.2d at 8. In *Roche*, the government had probable cause to believe the defendant was engaged in an extensive mail fraud scheme, systematically charging customers more for motor vehicle insurance. *Id*. at 7. The government obtained a warrant that authorized the seizure of books, records and documents "which are evidence, fruits, and instrumentalities of [mail fraud]." *Id.* The First Circuit found this limitation to be "no limitation at all," as the description did not limit the search to documents relating to motor vehicle insurance, but authorized the seizure of a far broader class of documents. *Id*. at 7–8.

232. *See supra* notes 226–31 and accompanying text; *see also* United States v. Lamport, 787 F.2d 474, 476 (10th Cir. 1986) (holding a warrant was sufficiently specific where statutory reference to the mail-fraud statute was limited by a list of medical records which were limited by patients and dates); *cf.* United States v. Spilotro, 800 F.2d 959, 964 (9th Cir. 1986) (holding a warrant violated the particularity requirement because it authorized wholesale seizures of entire categories of items which were not generally evidence of criminal activity, because it provided no guidelines to distinguish items used lawfully from those the government had probable cause to seize, and because it referred to a statute rather than particular criminal activities themselves).

233. *See* United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001).

234. 547 U.S. 90 (2006).

235. *Id*. at 97.

larity requirement.'"[236] Rather, the Amendment specifies the place to be searched and the persons or things to be seized are the only matters that must be particularly described in a warrant.[237]

The aforementioned particularity parameters do not merely satisfy "some general particularity requirement."[238] Courts have repeatedly held the government's failure to use information that further details a warrant's descriptions, if the government possesses or could obtain such information at the time of warrant application, will render a description of the items to be seized insufficient for purposes of the particularity requirement.[239] Failure to enforce the proposed parameters of particularity will result in warrants that give to the executing officers the task of determining which stored e-mails and files fall within the unnecessarily broad categories of items to be seized. Without limiting parameters, warrants fail to distinguish—or provide criteria for distinguishing—target communications from innocuous communications. Agents permitted to seize the entirety of a target-account will not consider their authority to be limited.[240] Focusing on the content of stored e-mails and files, identifying the parties to communications, restricting searches and seizures by relevant time frame, and recognizing a nexus between the communications sought and the crime committed is necessary to ensure warrants for stored e-mails are not akin to the colonial-era general warrants the particularity requirement prohibits.

C. Margin of Flexibility

While the number of files that may be scrutinized is not determinative, the seizure of all stored e-mails in an account is constitutionally justified only when *all* of those e-mails are within the scope of the probable cause underlying the warrant.[241] Rarely would this be the case—a target e-mail account will generally contain numerous e-mails which are completely irrelevant to a criminal investigation. Yet adherence to the particularity requirement does not always require that warrants be "elaborately detailed."[242] There may be instances when the government *does not* have information to establish parameters

236. *Id.*
237. *Id.*
238. *See id.*; *see also* Paul Ohm, Response, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 VA. L. REV. IN BRIEF 1, 10 (2011).
239. *See supra* note 159 and accompanying text.
240. United States v. Fuccillo, 808 F.2d 173, 177 (1st Cir. 1987); Montilla Records of P.R. v. Morales, 575 F.2d 324, 326 (1st Cir. 1978).
241. United States v. Hayes, 794 F.2d 1348, 1355 (9th Cir. 1986) ("The search and seizure of large quantities of material is justified if the material is within the scope of the probable cause underlying the warrant.").
242. United States v. Shoffner, 826 F.2d 619, 630 (7th Cir. 1987); *cf.* United States v. Kow, 58 F.3d 423, 427 (9th Cir. 1995) (holding a warrant that outlined fourteen

that limit the scope of a search and seizure, and it therefore may not always be possible to describe the sought-after e-mails or files with the aforementioned level of detail.

When assessing whether the level of detail is sufficiently particular, judicial officers must weigh the practical necessities of law enforcement against the likelihood of violating an individual's personal rights.[243] It is almost certain that a target e-mail account will contain stored communications both relevant and completely irrelevant to an investigation, and magistrate judges must therefore weigh heavily the likelihood that privacy will be violated if the aforementioned particularization is not implemented in the context of stored e-mail surveillance.[244] A greater degree of ambiguity may be tolerated, however, under certain circumstances.

1. Generic Descriptions When Information is Unavailable

A warrant authorizing a seizure of "any and all information and/or data" stored in an e-mail account should presumptively fail to satisfy the particularity requirement.[245] Such a categorical description is too broad in the sense it includes e-mails that should not be seized[246]—providing the government with unrestrained access to electronic records of one's daily activities and private affairs.[247] However, without some form of examination, it may be difficult for the government

categories of business records was insufficient because "the warrant contained no limitations on which documents within each category could be seized").

243. United States v. Cook, 657 F.2d 730, 733 (5th Cir. Unit A Sept. 1981).

244. *See* United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009) ("The modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement that much more important."); *In re* Lafayette Acad., Inc., 610 F.2d 1, 3–4 (1st Cir. 1979) (holding a warrant was insufficiently particular as it allowed seizure of nearly every book and document on premises of school, and as it created a likelihood of intermixture between a few "unlawful" and many "lawful" documents); United States v. Klein, 565 F.2d 183, 188 (1st Cir. 1977) (finding a warrant insufficient where it provided for the seizure of unlawful pirate tapes but where those tapes were likely to be mixed together with lawful tapes, and there was no indication of how they would be distinguished prior to seizure).

245. *See, e.g.*, *Otero*, 563 F.3d at 1132 ("[T]he government does not contest that a warrant authorizing a search of 'any and all information and/or data' stored on a computer would be anything but the sort of wide-ranging search that fails to satisfy the particularity requirement.").

246. *See* United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) ("The cases on 'particularity' are actually concerned with . . . whether the category as specified is too broad in the sense that it includes items that should not be seized.").

247. *See* United States v. Rosa, 626 F.3d 56, 61 (2nd Cir. 2010) (holding a warrant authorizing the search and seizure of any and all electronic equipment, digital files, and images "lacked meaningful parameters on an otherwise limitless search of Rosa's electronic media").

to know exactly which stored e-mail or file contains the sought-after content.[248] While this difficulty may, in theory, justify blanket-seizures of all stored e-mails and files contained in an account, the government must demonstrate to a magistrate judge *factually* why a broad search and seizure authority is reasonable; there must be some threshold-showing before the government may "seize the haystack to look for the needle."[249]

The use of a generic term or a general description of the stored e-mails and files, such as the "contents of all wire or electronic communications placed or entered in files controlled by the e-mail service provider,"[250] might be acceptable when further detail is unavailable, and a more precise description is impossible.[251] The government must demonstrate it did the best that could reasonably be expected under the circumstances, acquired all the descriptive facts which a reasonable investigation could uncover, and insured those facts were included in the warrant.[252] The government can demonstrate this by incorporating an affidavit by reference, explaining the government could not reasonably describe the targeted e-mails with more specificity into a warrant application.[253] Additionally, an explanatory affidavit docu-

248. United States v. Comprehensive Drug Testing, Inc. (*CDT II*), 621 F.3d 1162, 1176 (9th Cir. 2010) ("There is no way to be sure exactly what an electronic file contains without somehow examining its contents—either by opening it and looking, using specialized forensic software, keyword searching or some other such technique.").

249. *See* United States v. Hill, 459 F.3d 966, 975 (9th Cir. 2006) (rejecting the notion that the government "has an automatic blank check when seeking or executing warrants in computer-related searches").

250. A similar description was used in *Warshak v. United States*, No. 1:06-CV-357, 2006 WL 5230332, at *1 (S.D. Ohio July 21, 2006). *See also* United States v. Hanna, Nos. 09-1452, 09-2086, 2011 WL 3524292, at *4 (6th Cir. Aug. 12, 2011) (holding warrant authorized the seizure of "'[a]ll stored electronic mail of any kind sent to, from, and through [Dawn Hanna's AOL email account], or associated with the user name Dawn Hanna or account holder Dawn Hanna, between January 2001 and the present,' as well as business records and traffic data for that account").

251. *See* United States v. Leary, 846 F.2d 592, 602 n.13 (10th Cir. 1988); United States v. Timpani, 665 F.2d 1, 45 (1st Cir. 1981) ("[I]t is difficult to see how the search warrant could have been made significantly more precise."); United States v. Cook, 657 F.2d 730, 733 (5th Cir. Unit A Sept. 1981) (citing United States v. Cortellesso, 601 F.2d 28, 32 (1st Cir. 1979)); United States v. Dennis, 625 F.2d 782, 792 (8th Cir. 1980) (holding a warrant was as specific as circumstances would allow).

252. United States v. Buck, 813 F.2d 388, 590 (2nd Cir. 1987) (quoting United States v. Young, 745 F.2d 733, 759 (2nd Cir. 1984)).

253. *See Hill*, 459 F.3d at 976; United States v. Kow, 58 F.3d 423, 427 (9th Cir. 1995) ("Generic classifications in a warrant are acceptable only when a more precise description is not possible." (internal quotation marks and citation omitted)); *see also* United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) ("Of course, if the [seized] images themselves could have been easily obtained through an on-site inspection, there might have been no justification for allowing the seizure of *all*

ments the informed endorsement of the neutral, judicial officer issuing a warrant, an endorsement which is an essential safeguard that protects the privacy interests implicated by searches and seizures.[254]

However, such generic descriptions should be permitted only when those descriptions are shown to be related to an identified, specific, and illegal activity.[255] Otherwise, warrants authorizing blanket seizures of "any and all electronic communications" stored with an ISP would fail to satisfy the particularity requirement,[256] especially when there is no affidavit giving a reasonable explanation as to why a wholesale seizure is necessary.[257]

---

computer equipment, a category potentially including equipment that contained no images and had no connection to the crime.").

254. *Hill*, 459 F.3d at 976–77 ("The essential safeguard required is that wholesale removal must be monitored by the judgment of a neutral, detached magistrate." (citing United States v. Tamura, 694 F.2d 591, 596 (9th Cir. 1982))).

255. *See* United States v. Adjani, 452 F.3d 1140, 1148 (9th Cir. 2006) (providing that a warrant must tie the documents sought to the crimes alleged); Voss v. Gergsgaard, 774 F.2d 402, 406 (10th Cir. 1985) ("Where a warrant authorizes the seizure of particularly described records relevant to a specific crime and all of an organization's records, in fact, fall into that category, they may all lawfully be seized. However, a warrant that simply authorizes the seizure of all files, whether or not relevant to a specified crime, is insufficiently particular."); United States v. Federbush, 625 F.2d 246, 251 (9th Cir. 1980) (upholding the use of a search warrant that described the property to be seized generically as "documents, securities, papers . . . and . . . being held in violation of United States Code, Title 18, Section 2314" because it specified the crime and the enterprise to which the items listed were to pertain); United States v. McDarrah, 05 CR. 1182(PAC), 2006 WL 1997638 (S.D.N.Y. July 17, 2006), *cert denied*, 131 S. Ct. 80 (2010) (upholding a warrant which authorized the search of "[a]ll stored electronic mail and other stored content information presently contained in, or on behalf of, the following electronic mail addresses: Ps41alum@aol.com" because the affidavit extensively documented the continued use of the e-mail account in perpetrating the alleged crime, thereby establishing probable cause to search the entire e-mail account); *see also Cook*, 657 F.2d at 733 (discussing cases upholding warrants with generic descriptions).

256. *See* United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009) (holding a warrant authorizing seizure of "any and all information and/or data" failed the particularity requirement); United States v. Riccardi, 405 F.3d 852, 862 (10th Cir. 2005) (holding a warrant authorizing seizure of all storage media and "not limited to any particular files" violated the Fourth Amendment); United States v. Lacy, 119 F.3d 742, 746 (9th Cir. 1997) (explaining a warrant that contained "objective limits to help officers determine which items they could seize—allowing seizure only of documents linked to BAMSE, for example"); United States v. Fleet Mgmt. Ltd., 521 F. Supp. 2d 436, 443–44 (E.D. Pa. 2007) (holding a warrant that authorized a seizure of "any and all data . . . including but not limited to" a list of items turned a computer search warrant into an unconstitutional general warrant).

257. *See Hill*, 459 F.3d at 976; *Tamura*, 694 F.2d at 595 ("[T]he wholesale *seizure* for later detailed examination of records not described in a warrant is significantly more intrusive, and has been characterized as 'the kind of investigatory dragnet that the fourth amendment [sic] was designed to prevent.'" (quoting United States v. Abrams, 615 F.2d 541, 543 (1st Cir. 1980))).

2. Complex Criminality

The particularity requirement must also be applied with a practical margin of flexibility, taking into account the nature of the items to be seized[258] and the complexity of the case under investigation.[259] It has long been recognized that a criminal investigation requires investigators to piece together evidence that is often circumstantial and from multiple sources.[260] The Supreme Court has recognized a complex criminal investigation may require piecing together, "like a jigsaw puzzle," a number of evidentiary items that may not appear incriminating when taken alone.[261] Courts have justified a more flexible reading of the particularity requirement and upheld warrants permitting the seizure of all records pertaining to a certain offense when the crimes under investigation are complex and extensive.[262] This "pervasive fraud" doctrine permits an "all records" warrant where the affidavit supporting it demonstrates a pattern of illegal conduct that is likely to extend beyond the conduct already in evidence.[263] The doctrine is concerned with the breadth of the alleged criminality, i.e., whether evidence of criminal activity is likely to be found in a variety of records related to a wide range of activities.[264]

Thus, investigations for certain types of criminal activity may permit the government to deviate from its specificity obligation. For example, where the government establishes probable cause to believe that an e-mail account is used almost entirely or exclusively as part of a complex criminal endeavor, such as a pervasive scheme to defraud

258. *See, e.g.*, United States v. Riley, 906 F.2d 841, 845 (2d Cir. 1990) ("It is true that a warrant authorizing seizure of records of criminal activity permits officers to examine many papers in a suspect's possession to determine if they are within the described category. But allowing some latitude in this regard simply recognizes the reality that few people keep documents of their criminal transactions in a folder marked 'drug records.'"); United States v. Zanche, 541 F. Supp. 207, 210 (W.D.N.Y. 1982) ("Unlike other forms of property, business records are often incapable of being itemized one by one, particularly when their existence, but not their precise names or quantity, is all that is known.").

259. *See, e.g.*, Andresen v. Maryland, 427 U.S. 563, 481 n.10 (1976) ("Like a jigsaw puzzle, the whole 'picture' of petitioner's false-pretense scheme . . . could be shown only by placing in the proper place the many pieces of evidence that, taken singly, would show comparatively little."); United States v. Wuagneux, 683 F.2d 1343, 1349 (11th Cir. 1982); United States v. Regan, 706 F. Supp. 1102, 1113 (S.D.N.Y. 1989) ("The degree to which a warrant must state its terms with particularity varies inversely with [sic] complexity of the criminal activity investigated.").

260. United States v. Bradley, 644 F.3d 1213, 1259 (11th Cir. 2011).

261. *Andresen*, 427 U.S. at 481 n.10.

262. *See, e.g.*, United States v. Hargus, 128 F.3d 1358, 1362–63 (10th Cir. 1997) (upholding seizure of "any and all records relating to the business" under investigation for mail fraud and money laundering).

263. *Bradley*, 644 F.3d. at 1259.

264. *Id.*

or a drug conspiracy, all stored e-mail communications from the e-mail account could potentially be subject to seizure.[265] A description of the stored e-mails to be seized might then be sufficiently particular. If there is probable cause to believe that crime permeated the entire e-mail account, it would not be possible through a more specific description to separate stored e-mails that are evidence of the crime from those that are not.[266] Such a description leaves nothing to the discretion of the executing law-enforcement officers—they may seize all stored e-mails from the account.

Imagine, for example, that Roy is under investigation for conducting an "advance fee" scheme[267] and uses his e-mail account to conduct his allegedly fraudulent business. Law-enforcement agents submit an affidavit stating that—over the course of a two-year investigation and after speaking with multiple victims—the government concluded Roy had defrauded over 100 victims of more than five million aggregate dollars. The affidavit also describes how Roy conducted his fraudulent business via e-mail and provides extensive excerpts of e-mails sent from Roy's account to his victims. Because Roy's fraudulent business was primarily or solely criminal, and because Roy used his e-mail account as the primary e-mail account for conducting that business, there is likely sufficient evidence to establish probable cause that criminal activity permeated the e-mail account.[268]

---

265. *See, e.g.*, United States v. Kow, 58 F.3d 423, 427 (9th Cir. 1995) ("A generalized seizure of business documents may be justified if the government establishes probable cause to believe that the entire business is merely a scheme to defraud or that all of the business's records are likely to evidence criminal activity."); United States v. Sawyer, 799 F.2d 1494, 1508 (11th Cir. 1986) (stating that because the business was "permeated with fraud and . . . this fraud affected *all* [the defendant's] customers . . . the government . . . had no obligation to restrict the search to specific documents" where the evidence supported the broad search and seizure); United States v. Offices Known as 50 State Distrib. Co., 708 F.2d 1371, 1374 (9th Cir.1983), United States v. Brien, 617 F.2d 299, 305–09 (1st Cir. 1980) (upholding warrant for virtually all records of corporation where "the fraud was so extensive as to justify a belief by the magistrate that all these documents were likely to constitute evidence of the crimes under investigation").

266. *See* United States v. London, 66 F.3d 1227, 1238 (1st Cir. 1995) (noting where the defendant "operated a complex criminal enterprise where he mingled 'innocent' documents with apparently-innocent documents which, in fact, memorialized illegal transactions, . . . [it] would have been difficult for the magistrate judge to be more limiting in phrasing the warrant's language, and for the executing officers to have been more discerning in determining what to seize"); United States v. Kail, 804 F.2d 441, 445 (8th Cir. 1986).

267. *Common Fraud Schemes*, FED. BUREAU INVESTIGATION, http://www.fbi.gov/scams-safety/fraud (last visited Jan. 6, 2012). An "advance fee" scheme is a fraud through which victims are induced to pay money to someone in anticipation of receiving something of greater value but actually receive little or nothing in return. *Id.*

268. United States v. Bowen, 689 F. Supp. 2d 675, 683–84 (S.D.N.Y. 2010).

However, application of the "pervasive fraud" doctrine, or an extension of it, should be permissible *only* after investigating agents have demonstrated probable cause to believe a specific e-mail account is permeated with evidence of a complex crime.[269] Another example is illustrative: Imagine Dave works as a hedge fund manager at a financial firm. While most of Dave's business transactions have been legal, the government believes Dave used both his work and his personal e-mail accounts to perpetrate securities fraud. Dave sends and receives most of his business-related e-mails using his *work* e-mail address—most of Dave's e-mails related to both his legitimate and illegitimate business transactions are commingled in his work e-mail account. While the government could establish probable cause to seize all of the e-mails stored in Dave's work e-mail account, probable cause would *not* exist to validate a seizure of all e-mails stored in Dave's personal e-mail account.[270]

V. PRACTICALITIES OF PARTICULARITY

A search for and seizure of stored e-mails and files should extend no further than necessary to find the particular communications the warrant describes.[271] Requiring the government to provide the aforementioned level of detail protects privacy interests under the Fourth Amendment by preventing digital rummaging.[272] However, the execution of a warrant for physical evidence differs greatly from the execution of a warrant for stored data such as e-mail. Concerning the former, the government obtains a warrant to search a particular physical space for a particular piece of evidence, the government searches that space, and then the government seizes the evidence.[273] Executing a warrant for stored e-mail, however, flips the process. First, the warrant directs the ISP to produce *all* emails from the specified account or accounts.[274] After receiving a warrant, ISPs will typically

269. *See, e.g.*, *In re* Solid State Devices, Inc., 130 F.3d 853, 856–57 (requiring "a more substantial showing of pervasive fraud" where a company's business is primarily legitimate); *In re* Lafayette Acad., Inc., 610 F.2d 1, 5 (1st Cir. 1979) (holding a seizure of all records was not justified because defendant's business was legitimate and suspected criminal activity went to only one aspect of it).
270. United States v. Cioffi, 668 F. Supp. 2d 385, 387–89 (E.D.N.Y. 2009).
271. LAFAVE, *supra* note 101, at 551.
272. *See supra* Part IV.
273. *See* Orin S. Kerr, *Search Warrants in an Era of Digital Evidence*, 75 MISS. L.J. 85, 91 (2005).
274. *See* CCIPS SEARCH-AND-SEIZURE MANUAL, *supra* note 73, at 134; Kerr, *supra* note 273, at 91. The government may also subpoena the stored e-mail communications and files—ISPs ordinarily respond to such a subpoena by sending the government a computer disk containing the contents described in the subpoena. Kerr, *supra* note 8, at 1044. According to Kerr and others, while the government may not need a probable cause warrant to get a copy of the contents, it would need a warrant to access and search the contents for evidence. *Id*.

copy the information onto a storage drive, or print it out, and send it to the investigating agent.[275] Second, the warrant authorizes law enforcement to review the stored information to identify information that falls within the scope of the particularized items to be seized.[276]

The exact moment when a seizure of stored e-mails actually occurs is currently unsettled. However, many agree that such a seizure occurs when the government copies electronically stored data.[277] According to Orin Kerr, when the government makes a copy of electronic data it "adds to the information in the government's possession . . . which the government has not observed," constituting a seizure.[278] If copying the contents of stored e-mails amounts to a seizure, the government seizes that content when an ISP, acting as an agent of the government, makes a copy of the stored e-mail communications belonging to the target of the investigation.[279]

The stored e-mail seizure–search sequence is problematic due to a well-established exception to the warrant requirement. Under the plain view exception, the government may seize evidence that is in plain view without a warrant, provided that the government encounters this evidence during an authorized search and the incriminating nature of the evidence is "immediately apparent."[280] *United States v. Comprehensive Drug Testing, Inc.* (*CDT II*)[281] exemplifies how the plain view exception complicates the execution of a digital search and seizure. In *CDT II*, the government obtained a warrant for the drug-testing records of ten baseball players suspected of drug use.[282] Included in the warrant was a provision allowing the seizure of the drug-test records and the computers that contained the off-site examination.[283] When the government executed the warrant, the government seized and reviewed the drug-testing records for *hundreds* of players.[284] Although the government only had probable cause as to

275. *See* United States v. Bach, 310 F.3d 1063, 1066–68 (8th Cir. 2002).

276. *See id*.

277. *See, e.g.*, Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 MICH. TELECOMM. & TECH. L. REV. 39, 109 (2002); Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE L.J. 700, 714–15 (2010) (arguing that only copying of data that has not been exposed to human observation by a government agent amounts to a seizure).

278. Kerr, *supra* note 277, at 714.

279. *See* Smith v. Maryland, 442 U.S. 735, 740 n.4 (1979) (holding a telephone company was an "agent" of the police when it provided the pen register and the numbers recorded by the telephone company, thereby rendering "installation and use of pen register state action").

280. Horton v. California, 496 U.S. 128, 135–36 (1990) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971)).

281. 621 F.3d 1162 (9th Cir. 2010).

282. *Id*. at 1166.

283. *Id*. at 1168.

284. *Id*. at 1166.

ten players, it uncovered incriminating evidence of other individuals while reviewing all of the records, and it claimed that evidence was in plain view.[285]

Orin Kerr's particularity proposal—to which warrants simply naming the individual under investigation would be considered sufficiently particular—would essentially have the same effect.[286] Imagine the government establishes probable cause to believe Susan's e-mails contain evidence related to drug trafficking. In Kerr's view, the particularity requirement is satisfied if the government obtains a warrant to seize and subsequently search the contents of all of Susan's e-mail accounts.[287] The government serves the warrant on the various ISPs, and the ISPs hand over the contents of Susan's e-mail accounts to the government. Without further restrictions on the government, this situation presents the same problem the Ninth Circuit confronted in *CDT II*—the government can sift through a multitude of e-mails that are beyond the scope of the probable cause it has established.[288] If the government encounters incriminating evidence *not* related to drug trafficking, such evidence is in plain view.

To respond to the concern that his approach may "allow the government to sift through too many of an individual's communications, exposing a suspect's entire world of communications in plain view in a way that threatens to seem like a general warrant,"[289] Kerr proposes the elimination of the plain view exception for online searches.[290] Yet even Kerr acknowledges that eliminating the plain view exception would presently be too severe.[291] When presented with this proposal, members of the judiciary have argued against casting the plain view exception aside, allowing instead the incremental development of the contours of the plain view exception through the normal course of fact-based case adjudication.[292]

There is no need to require the government to foreswear reliance on the plain view exception in order to adhere to the Fourth Amendment. Stored e-mail warrants should describe the place to be searched and the things to be seized according to the aforementioned proposed standards of particularity—focusing on the content of sought-after e-mails and files. Particularity for stored e-mail warrants ensures nar-

285. *Id*. at 1170.
286. Kerr, *supra* note 8, at 1046.
287. *Id*.
288. *CDT II*, 621 F.3d at 1170.
289. Kerr, *supra* note 8, at 1047–48.
290. *Id*. at 1048 (citing Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 582–84 (2005) [hereinafter Kerr, *Searches and Seizures*]).
291. Kerr, *Searches and Seizures, supra* note 290, at 583.
292. United States v. Stabile, 633 F.3d 219, 241 n.16 (quoting United States v. Mann, 592 F.3d 779, 785 (7th Cir. 2010)).

row searches and seizures, thereby limiting them to a permissible scope and minimizing their intrusiveness.[293]

Where such detail is impossible and the description of the stored e-mails and files to be searched and seized becomes more general, "the method by which the search is executed becomes more important."[294] The "search method must be tailored to meet allowed ends,"[295] avoiding "transforming a limited search into a general one."[296] Yet it is precisely the process by which warrants for stored e-mail content are often executed that blocks adherence to the particularity requirement. Government agents ordinarily do not search through ISP's servers themselves.[297] Instead, the government serves a warrant on an ISP and the ISP produces the material specified in the warrant.[298] If a warrant authorizes the search and seizure only of the certain e-mails matching the warrant's descriptions, ISPs become the middlemen between the government and e-mail-account holders. On one hand, ISPs *should be* the middlemen. Requiring ISPs to segregate sought-after e-mails that are particularly described in warrants from those e-mails the government does not have probable cause to seize ensures constitutional reasonableness—the technical expertise of ISP technicians far outweighs that of law-enforcement officers, and the stored e-mails are located on the ISP's property.[299]

On the other hand, requiring ISPs to segregate e-mails identified in a warrant from those not identified may be burdensome and may create fear of liability if e-mails are improperly disclosed. However, this practical consideration does not counteract the constitutional requirement that warrants describe sought-after e-mails with particularity,[300] and ISPs do have specific forms of mitigating redress. First, the SCA shields ISPs from liability for compliance with the terms of a warrant that compels disclosure of stored e-mail communications.[301] Second, the SCA mandates the government reimburse ISPs that it compels to disclose stored e-mails for the costs incurred in searching, assembling, reproducing, and providing stored e-mail communica-

293. Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976).
294. United States v. Burgess, 576 F.3d 1078, 1094 (10th Cir. 2009).
295. *Id.*
296. *Id.*
297. CCIPS SEARCH-AND-SEIZURE MANUAL, *supra* note 73, at 134.
298. *Id.* (citing United States v. Bach, 310 F.3d 1063, 1068 (8th Cir. 2002) (finding search of email by ISP without presence of law enforcement did not violate Fourth Amendment)).
299. *Bach*, 310 F.3d at 1067 (utilizing these factors to find that the search of e-mail by ISP without presence of law enforcement did not violate Fourth Amendment).
300. *See* Bellia & Freiwald, *supra* note 8, at 176 (arguing the particularity requirement would be satisfied if the government compels disclosure only of those stored e-mails for which they have probable cause and service providers produce only those e-mails and related attributes that are particularly specified).
301. 18 U.S.C. § 2703(e) (2006 & Supp. III 2009).

tions.[302] This includes any costs incurred if the operations of the ISP's servers are disrupted.[303]

If ISPs prove unwilling, magistrate judges should impose restrictions on the government's execution of warrants for stored e-mail communications.[304] Mainly, examination of e-mail accounts and segregation of the stored e-mails particularly described in the warrant should be executed by a filter-team consisting of agents or specially-trained computer personnel or who are not involved in the investigation.[305] The filter-team should be prohibited from communicating to the investigating agents any information gleaned from e-mails and files not described in the warrant.[306] Once the e-mails, for which the government has probable cause to collect, have been isolated from other e-mails stored in an account, the investigating agents should be permitted to examine only the sought-after e-mails.[307] Such a restriction is necessary to prevent investigating agents from exercising unfettered discretion and to keep privacy intrusions to a minimum.[308] This is a "hardly revolutionary" solution to the problem of necessarily over-seizing evidence, offering the government a safe harbor to over-

302. *Id.* § 2706.

303. *Id*.

304. *See, e.g.*, United States v. Comprehensive Drug Testing, Inc. (*CDT II*), 621 F.3d 1162, 1168 (9th Cir. 2010).

305. *See id*. at 1172 ("[T]he representation in the warrant that computer personnel would be used to examine and segregate the data was obviously designed to reassure the issuing magistrate that the government wouldn't sweep up large quantities of data in the hope of dredging up information it could not otherwise lawfully seize."). The government can and does employ computer personnel to segregate documents before investigating agents gain access. *See, e.g.*, United States v. Vogel, No. 4:08-CR-224(1), 2010 WL 2268237, at *7 (E.D. Tex. May 25, 2010) ("[A] 'filter team' was established . . . [and] members of the investigation and prosecution teams did not view or rely upon privileged documents."). Orin Kerr has argued that ex ante restrictions on how warrants should be executed, such as requiring independent computer personnel to examine and segregate e-mails, have no legal effect because magistrate judges do not have the power to limit how warrants are executed beyond establishing the particularity of the place to be searched and things to be seized. Orin Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241, 1246 (2010). However, he also concedes that determining what may be seized is a core traditional function of magistrate judges reviewing warrant applications. *Id*. at 1263.

306. *See CDT II*, 621 F.3d at 1168–69.

307. *See id*.; United States v. Tamura, 694 F.2d 591, 595–96 (9th Cir. 1982) ("In the comparatively rare instances where documents are so intermingled that they cannot feasibly be sorted on site, we suggest that the Government and law enforcement officials generally can avoid violating fourth amendment [sic] rights by sealing and holding the documents pending approval by a magistrate of a further search . . . . The essential safeguard required is that wholesale removal must be monitored by the judgment of a neutral, detached magistrate.").

308. *See* Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976).

seize while simultaneously protecting privacy and property rights in stored e-mail communications.[309]

Some courts are hesitant to require that warrants specify the precise search method the government will use to uncover electronic data because limiting the government's search methodology ex ante would allow criminals to evade law-enforcement scrutiny by utilizing coded terms in their files or documents.[310] However, the process of segregating stored e-mails that may be seized from those which may not must not allow the government to access data which it has no probable cause to collect.[311] In many cases, utilizing a filter team will not compromise the government's ability to prosecute a case.[312] Additionally, the Supreme Court in *Dalia v. United States*[313] encouraged warrant applications that reveal the method of execution ex ante, calling this the "preferable approach."[314] Judicial officers alone delineate what may be seized pursuant to the warrant and what must be ignored, curtailing the discretion of the government in executing the warrant.[315] It is their duty to scrupulously impose restrictions on the government's electronic surveillance by tailoring authorization to conduct it.[316]

There is a far greater potential "for the 'intermingling' of documents" and "a consequent invasion of privacy" when police execute a

309. *CDT II*, 621 F.3d at 1178, 1180 (Kozinski, C.J., concurring).

310. *See, e.g.*, United States v. Hill, 459 F.3d 966, 978 (9th Cir. 2006) ("[T]here is no case law holding that an officer *must* justify the lack of a search protocol in order to support issuance of the warrant."); United States v. Brooks, 427 F.3d 1246, 1251 (10th Cir. 2005) ("At the outset, we disagree with [the defendant] that the government was required to describe its specific search methodology."); United States v. Upham, 168 F.3d 532, 537 (1st Cir. 1999) ("The . . . warrant did not prescribe methods of recovery or tests to be performed, but warrants rarely do so. The warrant process is primarily concerned with identifying *what* may be searched or seized—not how—and *whether* there is sufficient cause for the invasion of privacy thus entailed.").

311. *CDT II*, 621 F.3d at 1177.

312. *See In re* United States of America's Application for a Search Warrant to Seize and Search Electronic Devises from Edward Cunnius, 770 F. Supp. 2d 1138, 1150 (W.D. Wash. 2011); CCIPS SEARCH-AND-SEIZURE MANUAL, *supra* note 73, at 80 ("[P]rosecutors should oppose such restrictions whenever they significantly interfere with the government's ability to obtain evidence that falls within the scope of the warrant.").

313. 441 U.S. 246 (1979).

314. Ohm, *supra* note 238, at 3–4.

315. Marron v. United States, 275 U.S. 192, 196 (1927) (stating the particularity requirement "prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant").

316. *See* United States v. Cox, 449 F.2d 679, 687 & n.14 (10th Cir. 1971) ("In tailoring an authorization the judge might well require, for example, early and frequent reports in writing by the officer as to the nature and character of the interceptions, whereby further specific orders could be imposed.").

search for electronically-stored evidence.[317] Due to the intrusiveness of searching and seizing the contents of stored e-mails and files, magistrate judges should place restrictions on the execution of warrants to ensure adherence to the Fourth Amendment.[318] Requiring segregation of the sought-after communications from those which the government has no probable cause to seize is within the power of magistrate judges, a power to limit how warrants are executed and a power to ensure adherence to the particularity requirement.[319] Placing limits on the execution of warrants for stored e-mails ensures the particularity requirement is checked by judges, not by the police themselves.[320] Without such a neutral predetermination of the scope and breadth of stored e-mail searches and seizures, individuals are secure from Fourth Amendment violations only at the discretion of police.[321]

VI. CONCLUSION

The law of electronic surveillance, as it currently stands in most jurisdictions, permits the government to search and seize stored e-mails and files in violation of the particularity requirement of the Fourth Amendment. The privacy implications of such overly broad searches and seizures necessitate that warrants to search and seize stored communications adhere to the Amendment's particularity requirement. Searching and seizing stored emails pursuant to warrants that do not describe the place to be searched and things to be seized with particularity will result in digital rummaging. The Fourth Amendment requires more. The standards set forth in this Article guide the application of the particularity requirement to stored e-mail surveillance and help strike the proper balance between law enforcement's need to investigate crime and the individual's right to maintain some semblance of privacy in the face of rapidly-advancing surveillance technologies. The Fourth Amendment demands the standards set forth in this Article, ensuring that warrants for stored communication surveillance describe with particularity the place to be searched and the communications to be seized—a constitutional precondition on this method of electronic surveillance.[322]

317. *See* United States v. Lucas, 640 F.3d 168, 178 (6th Cir. 2011).
318. *See* United States v. Payton, 573 F.3d 859, 864 (9th Cir. 2009).
319. *See* Kerr, *supra* note 305, at 1246; *see also* Katz v. United States, 389 U.S. 347, 356–57 (1967) ("[The agents] were not compelled, during the conduct of the search itself, to observe precise limits established in advance by a specific court order . . . . In the absence of such safeguards, this Court has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end.").
320. *Cf.* Kerr, *supra* note 8, at 1042 (citing *Katz*, 389 U.S. at 359).
321. *Cf. Katz*, 389 U.S. at 358–59 (quoting Beck v. Ohio, 379 U.S. 89, 97 (1964)).
322. *Cf. id.*